DPS Telecom

"Your Partners in Network Alarm Monitoring"

NetGuardian 420

HARDWARE USER MANUAL

Visit our website at www.dpstelecom.com for the latest PDF manual and FAQs.

September 8, 2015 **D-UM-NG420** **Firmware Version 5.2G**

Revision History

Septemeber 8, 2015	DNP - Update
August 4, 2015	DNP - Points list
May 12, 2015	DNP - DWire Updates
January 26, 2015	Added DNP3 Section
January 28, 2014	Changed SSH screenshot and verbage
January 10, 2014	Edited TTY and SSH login information
December 3, 2013	Removed PPP Configuration
October 28, 2013	Added CellGuard Option
June 13, 2013	Added SCAN protocol support
April 9, 2013	Added D-Wire support
March 27, 2013	Added SSH via PuTTY Information
June 25, 2012	Added Hinged Pluggable Back Panel and Switch TestBox to Optional Accessories
June 19, 2012	Updated new web interface and build options. Division of Hardware and Web into separate manuals - FW version 1.1A and after
March 2, 2012	Edited relay information
March 9, 2011	Included Web Interface section
March 3, 2011	Included information about the wire wrap attachment option
September 21, 2010	Updated Shipping and Accessories Lists
August 19, 2010	Misc. user manual edits.

This document contains proprietary information which is protected by copyright. All rights are reserved. No part of this document may be photocopied without prior written consent of DPS Telecom.

All software and manuals are copyrighted by DPS Telecom. Said software and manuals may not be reproduced, copied, transmitted or used to make a derivative work, by either mechanical, electronic or any other means in whole or in part, without prior written consent from DPS Telecom, except as required by United States copyright laws.

© 2015 DPS Telecom

Notice

The material in this manual is for information purposes and is subject to change without notice. DPS Telecom shall not be liable for errors contained herein or consequential damages in connection with the furnishing, performance, or use of this manual.

Parts List:

Please make sure all of the following items are included with your NetGuardian 420. If parts are missing, or if you ever need to order new parts, please refer to the part numbers listed and call DPS Telecom at 1-800-622-3314.

Resource CD

DB9 Download Cable

Ethernet Cable

x 8

3/8" Ear Screw

x 4

Metric Rack Screw

x 4

Standard Rack Screw

x 2 (Single Input)
x 3 (Dual Input)

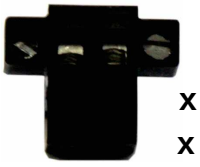
3/4 Amp Fuse

x 2

19" Rack Ear

x 2

23" Rack Ear



x 1 (Single Input)
x 2 (Dual Input)

Main Power Connector

x 2

Cable Tie

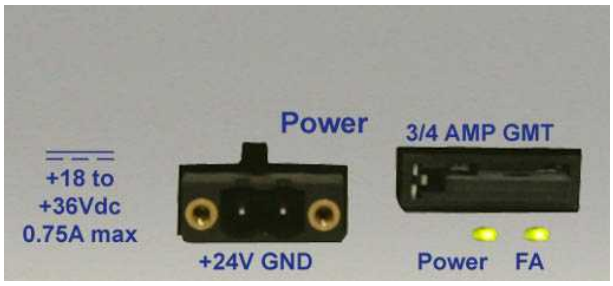
Pad

Telephone Cable (Optional)

SETUP: Parts List

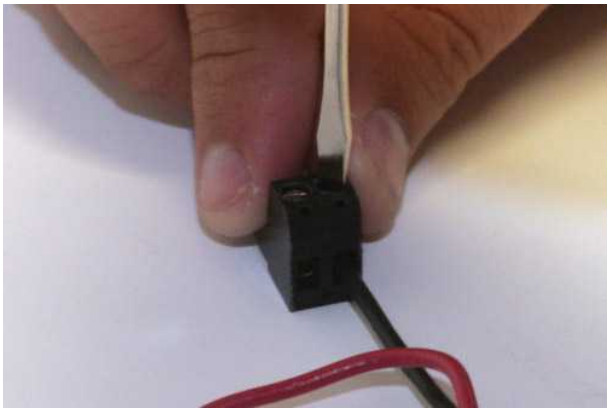
SETUP: Powering the Device

Powering the Device:



FA LED Fuse left, power status LED , power plug right

1) Insert a battery ground wire into the connector's right terminal (Shown below) and battery lead into the left terminal and tighten the screws. Insert the connector into the power plug. Attach a grounding wire to the grounding lug.



Battery lead left, and Ground right

1) Insert a battery ground wire into the connector's right terminal (Shown above) and battery lead into the left terminal and tighten the screws. Insert the connector into the power plug. Attach a grounding wire to the grounding lug .

2) Ensure the power status LED is lit up green for correct polarity.

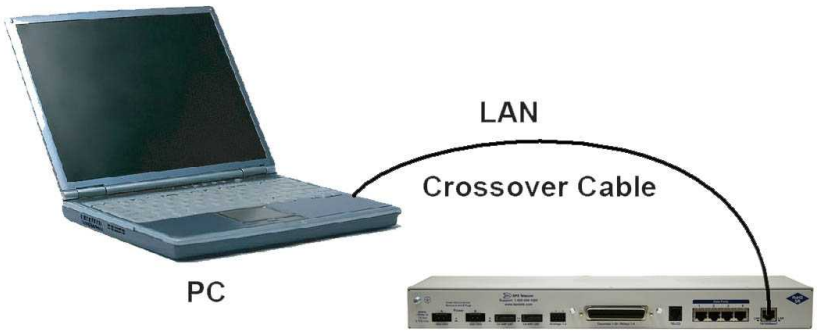
3) Insert the local fuse into the fuse holder.

4) The front panel status LED should flash RED and GREEN to indicate that the unit is operating.

Note: Always use safe power practices when making power connections. Make sure the power wires are not active before making any power connections.

Connect via LAN:

1) Connect PC and the NetGuardian device to the same network via switch or directly via LAN cable.

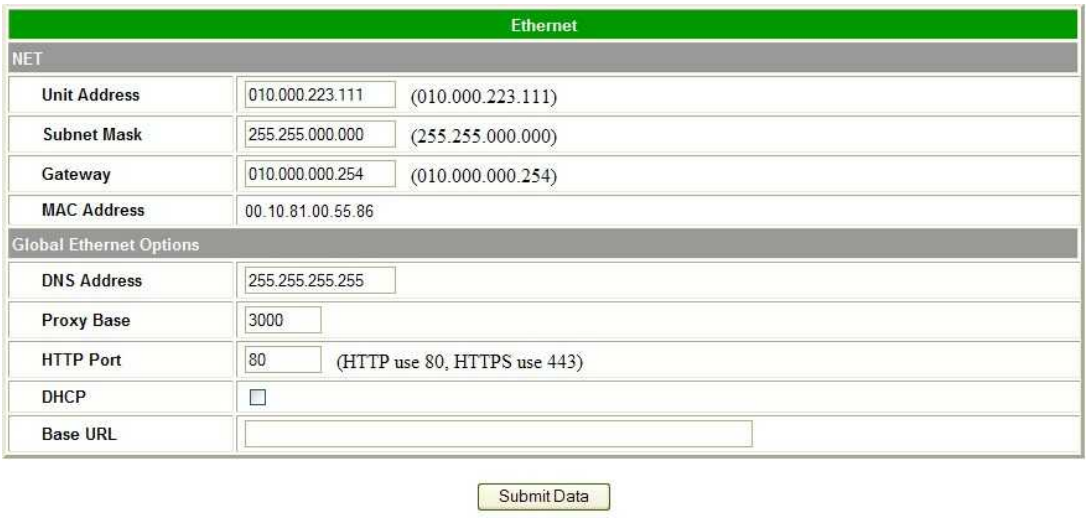


2) Record your PC's current IP configuration (especially if static assignment).

3) Set your PC's IP address to 192.168.1.200 and subnet mask to 255.255.255.0 (Contact your IT department if you are unsure how to do this).

4) Browse to 192.168.1.100 (Compatible with IE8 or greater) on your PC and log in with default user:admin and password:dpstelecom. Click "Edit" and then "Ethernet" to bring up the next menu.

5) Provision the NetGuardian with the appropriate IP information for your network and restart the unit. Then restore your computer's IP configuration.



SETUP: Connect via LAN

SETUP: Test Email Notification

Test Email Notification:

1) Click on the "Edit" -> "Notifications" button in the Provisioning. You can set as many as 8 notifications. In this example, we'll setup Notification 2 to send emails.

Notification

ID	Type	Phone/Domain	Pin/Rcpt/Port	Baud/WFmt		IPA	Group
1	SNMPv1			9600	8,N,1	126.010.230.170	0
2	Off			1200	7,E,1	255.255.255.255	0
3	SNMPv1			1200	7,E,1	255.255.255.255	0
4	Off			1200	7,E,1	255.255.255.255	0
5	Text			1200	7,E,1	255.255.255.255	0
6	Off			1200	7,E,1	255.255.255.255	0
7	Off			1200	7,E,1	255.255.255.255	0
8	Off			1200	7,E,1	255.255.255.255	0

Submit Data

2) Under the Type column, select Email from the drop-down menu.

3) Enter the domain name of the email address under the Phone/Domain heading. This is the portion of an email address after the @ symbol in name@domain.com.

4) Enter the email recipient's user name under the PIN/Rcpt/Port heading. This is the portion of an email address before the @ symbol in the name@domain.com.

5) Enter the IP address of the SMTP mail server in the IPA field.

Notification

ID	Type	Phone/Domain	Pin/Rcpt/Port	Baud/WFmt		IPA	Group
1	Email	dpstele.net	johndoe	1200	7,E,1	123.123.123.1	0

6) Click Submit Data to save your email notification settings.

7) To set up the "from" address sent in email messages, click on the System link. Entering the appropriate information in the "Name" and "Location" fields. The email notification from the NetGuardian will appear as follows: name@location. (Ex. NetGuardian420@dpstele.net shown below)

System

Name	NetGuardian420
Location	dpstele.net

8) Click Submit Data to save your new system information settings.

Congratulations! Your notifications are configured and your NetGuardian 420 is live.

Contents

Visit our website at www.dpstelecom.com for the latest PDF manual and FAQs

1 NetGuardian 420 Overview 1

2 Shipping List 2

3 Optional Accessories 3

4 Specifications 4

5 Hardware Installation 5

5.1 Tools Needed 5

5.2 Mounting 5

5.3 Power Connection 6

5.4 LAN Connection 7

5.5 Telco Connection 7

5.6 Alarm and Control Relay Connections 8

5.6.1 Alarm and Control Relay Connector Pinout Table 8

5.6.2 Discrete Inputs/Control Relay Pinout 9

5.6.3 Optional Wire Wrap Back Panel 10

5.6.4 Integrated Temperature and Battery Sensor (Optional) 11

5.7 Discrete Alarms 12

5.8 Data Ports 13

5.9 Optional 66 Block Connector 14

5.10 Controls 15

6 LCD Display 16

6.1 Alarm and Control Status Messages 16

6.2 LCD Command Menu 17

6.2.1 Sound off 17

6.2.2 Reboot 18

6.2.3 Run Config 18

6.2.4 Contrast 18

7 Alarm Speaker 19

8 Front Panel LEDs 20

9 Back Panel LEDs 20

10 Configuring the NetGuardian 21

10.1 RADIUS Authentication 21

11 Connecting to the NetGuardian 22

11.1 ... via Craft Port 22

11.2 ... via LAN 23

12 TTY Interface 24

12.1 Unit Configuration 24

12.1.1 Ethernet Port Setup 24
12.1.2 Edit PPP Port 26
12.1.3 Tune 202 Modem 27
12.1.4 RADIUS Configuration 28
12.1.5 New! - TTY Command Mode 29
12.2 Monitoring 32
12.2.1 Monitoring the NetGuardian 32
12.2.1.1 Monitoring Base Alarms 32
12.2.1.2 Monitoring Ping Targets 33
12.2.1.3 Monitoring and Operating Relays (Controls) 33
12.2.1.4 Monitoring Analogs 34
12.2.1.5 Monitoring System Alarms 35
12.2.1.6 Monitoring Data Port Activity 36
12.2.1.7 Monitoring the Accumulation Timer 36
12.2.2 Viewing Live Target Pings 37
12.2.3 Proxy Menu 38
12.2.4 Event Logging 38
12.2.5 Backing Up NetGuardian Configuration Data via FTP 39
12.2.5.1 Reloading NetGuardian Configuration Data 39
12.2.6 Debug Input and Filter Options 40
13 Web Interface 41
13.1 Logging on to the NetGuardian 41
13.2 Navigating the Web Interface 42
13.3 Edit Mode 42
13.3.1 System Settings 43
13.3.2 Defining SNMP Parameters 44
13.3.3 Controlling Access to the NetGuardian 47
13.3.3.1 Logon Settings 47
13.3.3.2 Logon Profiles and Access Rights 47
13.3.3.3 Filter IPA Config and Operation 49
13.3.3.4 Radius Authentication Settings 50
13.3.4 Ethernet Settings 51
13.3.4.1 Using the Base URL Field 51
13.3.5 Configuring Ports 53
13.3.5.1 Modem Settings 53
13.3.5.2 Data Port Settings 54
13.3.5.2.1 Data Port Types 55
13.3.5.2.2 Direct and Indirect Proxy Connections 56
13.3.6 Configure Alarm Notifications 57
13.3.6.1 Alphanumeric Pager Setup 58
13.3.6.2 SNPP Notification Setup 58
13.3.6.3 Numeric Pager Setup 58

13.3.6.4 Text Paging Setup 59
13.3.6.5 Email Notification Setup 59
13.3.6.5.1 SMTP & POP3 Authentication Support 60
13.3.6.6 SNMPv1 Paging Setup 60
13.3.6.7 SNMPv3 Paging Setup 60
13.3.6.8 TCP Paging Setup 61
13.3.6.9 NUM17 Pager Setup 62
13.3.6.10 Echo Notification Setup 62
13.3.7 Defining Point Groups 63
13.3.8 Configuring Base Discrete Alarms 64
13.3.9 Configuring System Alarms 65
13.3.10 Setting Ping Targets 66
13.3.11 Setting the Accumulation Timer 67
13.3.12 Configuring Analogs 68
13.3.12.1 Integrated Temperature and Battery Sensor (Optional) 69
13.3.12.2 Analog Polarity Override 69
13.3.12.3 Analog Step Sizes 70
13.3.13 Configuring Control Relays 70
13.3.14 Setting Event Qualification TImers 71
13.3.15 Setting System Timers 72
13.3.16 Setting the System Date and Time 74
13.3.16.1 Network Time Protocol Support 75
13.3.17 PPP Modes 75
13.3.18 Building Access Control 77
13.3.19 Configuring IP Cameras 78
13.3.20 Alarm Sync 79
13.3.21 Saving Changes or Resetting Factory Defaults 79
13.3.21.1 Rebooting the NetGuardian 79
13.4 Monitor Mode 80
13.4.1 Alarm Summary 80
13.4.2 Base Alarms 80
13.4.3 Ping Targets 80
13.4.4 Base Analogs 81
13.4.5 System Alarms 81
13.4.6 Accum Timer 81
13.4.7 Controls 82
13.4.8 Event Log 82
13.4.9 Monitoring Port Activity 83
14 Reference Section **84**
14.1 Display Mapping 84
14.1.1 System Alarms Display Map 85

14.2 SNMP Manager Functions 88
14.3 SNMP Granular Trap Packets 89
14.4 Trap SNMP Logic 90
14.5 ASCII Conversion 90
14.6 RADIUS Dictionary File (Available on Resource Disk) 91
14.7 DNP3 Configuration / Interoperability Guide 92
14.7.1 DNP v3.0 Device Profile 92
14.7.2 DNP V3.0 Implementation Table 95
14.7.3 DNP V3.0 Point List 96
15 Frequently Asked Questions 100
15.1 General FAQs 100
15.2 SNMP FAQs 103
15.3 Pager FAQs 104
16 Technical Support 105
17 End User Iisence Agreement 106

1 NetGuardian 420 Overview

The NetGuardian has all the tools you need to manage your remote site.

The NetGuardian 420 - The Intelligent RTU for Complete Site Management
The NetGuardian 420 is a RoHS 5/6-compliant, LAN-based, SNMP/DCPx remote telemetry unit. The NetGuardian has all the tools you need to manage your remote sites, including built-in alarm monitoring, paging and email capabilities that can eliminate the need for an alarm master.

With the NetGuardian, you can:

- Monitor 20 discrete alarms, 32 ping alarms, and up to 6 analog alarms
- Control remote site equipment via 4 terminal server ports and up to 4 control relays
- Monitor your remote site from anywhere using the NetGuardian's built-in Web Browser Interface.
- Report alarms to multiple SNMP managers or the T/Mon NOC Alarm Monitoring System.
- Report alarms via LAN or dial-up connection.
- Automatically send pager and email alarm notifications 24/7.
- Connect multiple concurrent users via Telnet over LAN to telecom switches, servers, radios, PBXs and other equipment.
- Monitor discrete and analog threshold alarms.
- Ping IP network devices and verify that they're online and operating.

New: The NetGuardian 420 supports serial baud rates up to 115,200, **optional** external temperature sensor, analog readings accurate to within +/- 1%, one 10/100 NICs (isolated), SNMPv2c, SNMPv2c Inform trap, and SNMPv3.

Stand-alone local visibility
You don't need an alarm master unit to monitor your site with the NetGuardian. With the NetGuardian's built-in Web Browser Interface, you can access the NetGuardian, view alarms and control remote site devices from any computer anywhere in your network.

24/7 pager and email alerts - no master needed
Out of the box, the NetGuardian supports 24/7 pager and email reporting. Send alarms directly to maintenance technicians in the field, even when no one's in the office.

Connect via LAN to telecom switches, servers, radios and more
Each of the NetGuardian's eight serial ports can be individually configured to serve as a craft port, a channel port or a TCP or UDP reach-through port, giving you LAN-based terminal server access to up to 4 serial devices.

NEW - RADIUS Authentication
Take the security of your alarm remotes to the next level with RADIUS authentication. Now the NetGuardian 420 can interact with your RADIUS server, integrating it as part of your enterprise management.

Reports to multiple SNMP managers and T/Mon NOC simultaneously
The NetGuardian reports to both the T/Mon NOC Alarm Monitoring System and any SNMP manager. You can simultaneously forward alarms from the NetGuardian to T/Mon NOC and multiple SNMP managers at multiple IP addresses. Alarms can also be configured to dispatch to one, some, or all SNMP managers.

2 Shipping List

While unpacking the NetGuardian, please make sure that all of the following items are included. If some parts are missing, or if you ever need to order new parts, please refer to the part numbers listed and call DPS Telecom at **(800) 622-3314**.

NetGuardian 420: D-PK-NG420

NetGuardian 420 Hardware Manual D-UM-NG420

NetGuardian 420 Resource CD (includes manuals, MIBs, and software)

DB9M-DB9F Download Cable 6 ft. D-PR-045-10-A-04

One Ethernet Cables 14 ft. D-PR-923-10A-14

x2

23" Rack Ears D-CS-325-10A-01

x2

19" Rack Ears D-CS-325-10A-00

x4

Four Metric Rack Screws 2-000-80750-03

x8

Eight 3/8" Ear Screws 1-000-60375-05

x4

Four Standard Rack Screws 1-000-12500-06

Power Connector Plugs for Main Power Fuses 2-820-35102-00

x3

Three 3/4-Amp GMT Main Power

2-741-00750-00

x2

Two Cable Ties

Pads
2-015-00030-00

Screws and connectors are packaged in a sealed hardware kit, shown above

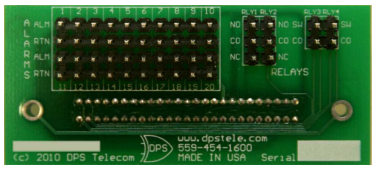
(Hardware kit containing a WAGO connector)

3 Optional Accessories

Telephone Cable 6 ft.
(Optional, if ordering modem)
D-PR-045-10A-01

4 Pin Analog Connector
(optional, for analogs)
2-820-00814-02

External Temperature Sensor
D-PR-1870-10A-07



Wire Wrap Back Panel
D-PK-WWADP-12003.00001

NetGuardian SiteMON IP G2 **D-PK-CAMRA**

The NetGuardian SiteCAM provides streaming video security surveillance of remote sites. The SiteCAM connects to either the NetGuardian's integrated 10/100BaseT switch or a separate 10/100/1000 switch. SiteCAM video can be accessed directly from the NetGuardian's Web Browser Interface. Up to four cameras can be supported.

4 Specifications

Discrete Alarm Inputs:	20
Analog Alarms:	Up to 6 2 user defined / 1 Internal temp / 1 External temp / 2 Voltage)
	Analog Input Range: (–94 to 94 VDC or 4 to 20 mA)
Control Relays:	**4** (2 Form A and 2 Form C)
	Maximum Voltage: 60 VDC/120 VAC
	Maximum Current: 1 Amp, AC/DC
Ping Alarms:	32
Protocols:	SNMPv1, SNMPv2c, SNMPv3, DCPx, DCPf, TRIP, SNPP
	SMTP, TAP, HTTP, FTP, TELNET, ICMP, RADIUS
Interfaces:	4 RJ45 Yost serial ports
	1 RJ45 10/100 Ethernet ports
	1 RJ11 telco jack (optional for modem)
	1 50-pin amphenol connectors (discretes, controls, and analogs)
	1 4-pin screw connector (analogs)
Dimensions:	1.75"H x 17"W x 7.5"D
Mounting:	19" or 23" rack
Weight:	3.5 lbs
Power Input:	–48VDC (–36 to –72 VDC)
	(Optional) –24 VDC (–18 to –36 VDC)
	(Optional) Wide Range –24/–48 VDC (–18 to –58 VDC)
`	(Optional) +24VDC (+18 to +36VDC)
Power Output:	(Optional) +12 VDC or +24 VDC power output for external sensor
Current Draw:	500 mA at 48VDC
Fuse:	3/4 amp GMT for power inputs
Modem:	33.6 K internal (optional)
Visual Interface:	LCD display
	9 bicolor LEDs
	5 unicolor LEDs
Audible Notification:	Alarm speaker
Operating Temperature:	32°–140° F (0°–60° C)
Operating Humidity:	0%–95% noncondensing
Build Options:	Real-time clock, HTTPS (Secure web browsing), Serial port options: RS232, RS485, or 202 modem
MTBF:	60 years
Windows Compatibility:	Windows 95, 98 NT, ME, XP, 2000, Vista, 7 32/64 bit
RoHS:	5/6

5 Hardware Installation

5.1 Tools Needed

To install the NetGuardian, you'll need the following tools:

Phillips No. 2 Screwdriver

Small Standard No. 2 Screwdriver

Wire Strippers/Cutter

Wire Wrap Gun (if hinged wire wrap panel is used)

Punch Down Tool (if 66 blocks are used)

PC with terminal-emulating software (i.e. HyperTerminal)

5.2 Mounting

The NetGuardian can be flush or rear-mounted

The NetGuardian mounts in a 19" rack or a 23" rack using the provided rack ears for each size. Two rack ear locations are provided. Attach the appropriate rack ears in the flush-mount or rear-mount locations shown in Figure 6.2.1.

Note: Rack ears can be rotated 90° for wall mounting or 180º for other mounting options (not shown).

5.3 Power Connection

Power connectors and fuses.

The NetGuardian has two screw terminal barrier plug power connectors, located on the left side of the back panel.

> **The Grounding Lug on the back of the unit provides a permanent connection to earth ground when connected. The Grounding Lug must be used in order to comply with standards.**

Before you connect a power supply to the NetGuardian, test the voltage of your power supply:

- Connect the black common lead of a voltmeter to the ground terminal of the battery, and connect the red lead of the voltmeter to the battery's –48 VDC terminal. The voltmeter should read **between –43 and –53 VDC**. If the reading is outside this range, test the power supply.

To connect the NetGuardian to a power supply, follow these steps:

1. Remove the fuse from the back panel of the NetGuardian. **Do not reinsert the fuse until all connections to the unit have been made.**

2. Remove the power connector plug from Power Connector A. Note that the plug can be inserted into the power connector only one way - this ensures that the barrier plug can only be reinserted with the correct polarity. Note that the **–48V terminal is on the left** and the **GND terminal is on the right**.

3. Use the grounding lug to connect the unit to earth ground. The grounding lug is next to the ⏚ symbol. Insert the eyelet of the earth ground cable between the two bolts on the grounding lug (Ground cable not included).

4. Insert a **battery ground** into the power connector plug's **right terminal** and tighten the screw; then insert a **–48 VDC** line to the plug's **left terminal** and tighten its screw.

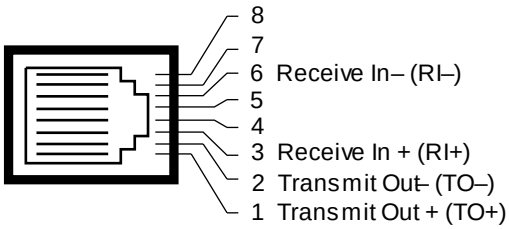
5. Push the power connector plug firmly back into the power connector. If the power feed is connected correctly, the LED by the connector will light **GREEN**. If the polarity of the power feed is reversed, the LED will not illuminate.

6. Repeat Steps 2–4 for Power Connector B.

7. Reinsert the fuse to power the NetGuardian. The front panel LEDs will flash **RED** and **GREEN**.

5.4 LAN Connection

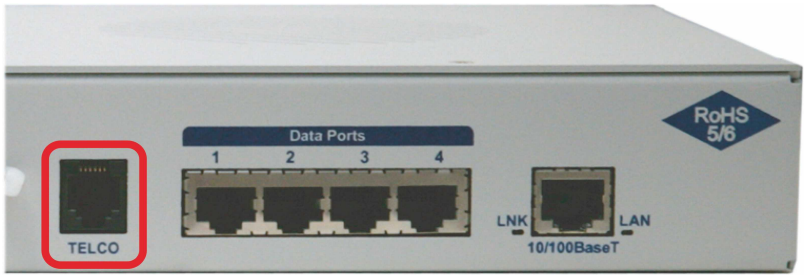
RJ45 Ethernet Connection



Ethernet port pinout

For enhanced security, the NetGuardian 420 has one 10/100 Ethernet ports. If the IP connection is OK, the LNK LED will light **SOLID GREEN** when the cable is connected.

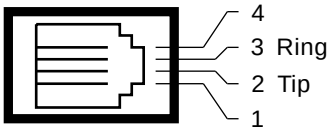
5.5 Telco Connection



Telco jack

The rear panel telco jack connects the NetGuardian's internal 33.6 modem to a standard phone line for dial-up access and pager alarm notification.

RJ11 Phone Line Connection



Pinout for the Telco jack

5.6 Alarm and Control Relay Connections

*Alarm and control relay connectors (*Optional Analog Connector Shown)*

The NetGuardian 420's discrete alarm inputs, control relay outputs are connected through the 50-pin connectors labeled "Discretes 1–20/ Relays 1–4" on the back panel. Analog alarm inputs 1 and 2 are connected through the four-pin analog connector.

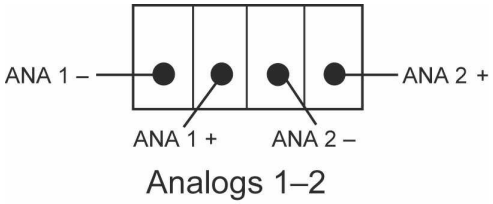
Note: Analog alarms are a build option for the NetGuardian 420. Your NetGuardian 420 may not have analog inputs.

5.6.1 Alarm and Control Relay Connector Pinout Table

Discretes 1–25					
	RTN	ALM		RTN	ALM
ALM 1	1	26	**ALM 13**	13	38
ALM 2	2	27	**ALM 14**	14	39
ALM 3	3	28	**ALM 15**	15	40
ALM 4	4	29	**ALM 16**	16	41
ALM 5	5	30	**ALM 17**	17	42
ALM 6	6	31	**ALM 18**	18	43
ALM 7	7	32	**ALM 19**	19	44
ALM 8	8	33	**ALM 20**	20	45
ALM 9	9	34			
ALM 10	10	35			
ALM 11	11	36			
ALM 12	12	37			

Control Relays 1–4			
	NO	NC	CO
CTRL 1	21	46	47
CTRL 2	23	48	22
***CTRL 3**	49	49	24
***CTRL 4**	50	50	25

Analogs 1–2		
ADC	–	+
1	1–	1+
2	2–	2+

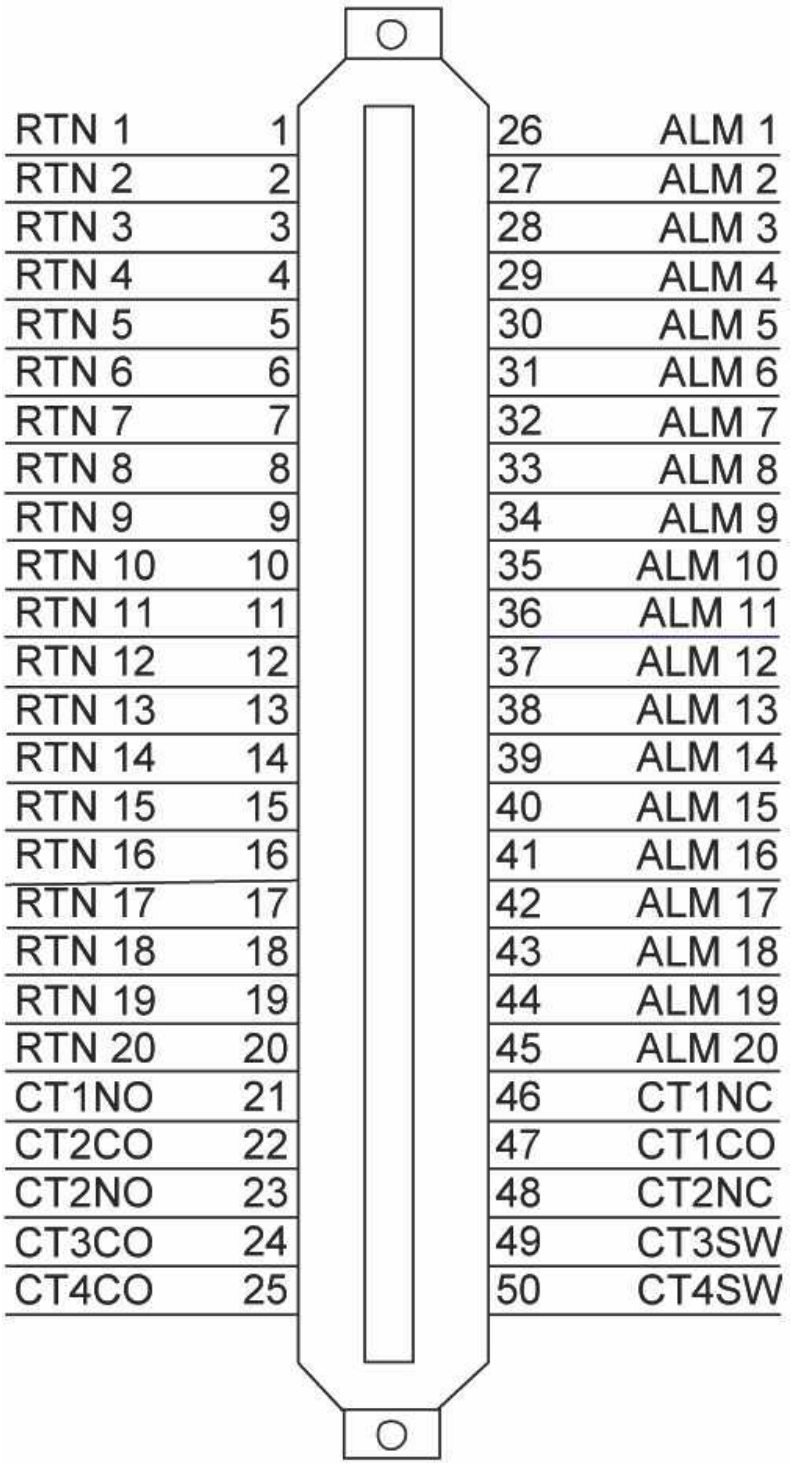


Alarm and control relay connector pinout for the 420

Above, you'll see pinouts for the 50-pin connector "Discretes 1–20 / Relays 1–4," and the pinout for the four-pin connector "Analogs 1–2."

***You can set your NetGuardian's control relays 3 and 4 for either Normally Open or Normally Closed operation via a jumper on the NetGuardian PC board. By default, relays 3 and 4 are configured for Normally Open operation. For more information, see the **Controls** section of this manual.

5.6.2 Discrete Inputs/Control Relay Pinout



Pinout of the NetGuardian Amphenol labeled "Discretes 1-20/Relays 1-4"

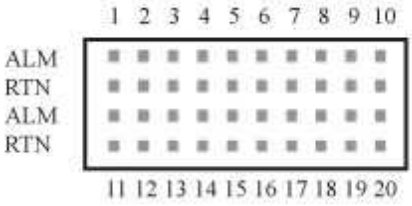
Note: CT3SW and CT4SW indicate relays 3 and 4, which are hardware configurable (switched) for Normally Open or Normally Closed operation via jumpers on the NetGuardian PC Board. By default, relays 3 and 4 are set for Normally Open operation.

5.6.3 Optional Wire Wrap Back Panel

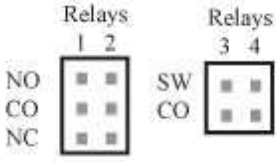
The Wire Wrap attachment for the NetGuardian 420

The optional wire wrap attachment provides wire-wrap connections for the NetGuardian 420's alarms and control relays. To connect alarms and relays to the back panel:

1. Connect the panel directly to the unit's rear amphenol.
2. Connect discretes and control relays to the appropriate pins.



Pinout for the Wire Wrap Discrete Alarms



Pinout for Wire Wrap Control Relays

5.6.4 Integrated Temperature and Battery Sensor (Optional)

The external temperature sensor

The optional integrated temperature and battery sensor monitors the ambient temperature and the NetGuardian's power inputs. This option is available only if it was ordered with your NetGuardian. The integrated temperature sensor measures a range of 32° F to 140° F (0° C to 60° C) within an accuracy of ± 1°.

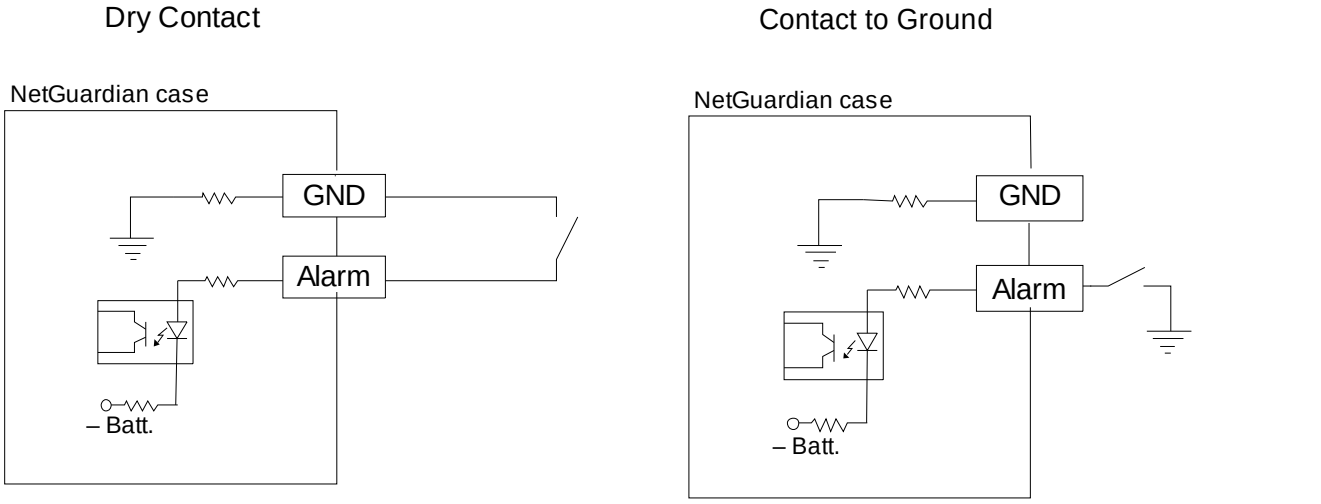
Sensor Function	Analog Input Options
Temperature	Can be used on analog input 7 (Internal)
Power Feed A	Can be used on analog input 5
Power Feed B	Can be used on analog input 6
Temperature	Can be used on analog input 8 (External)

Integrated sensor connection options

Each integrated sensor takes the place of an analog input, and does not need any external connections. No other analog input can be connected to the input point used for the integrated sensors. The table above lists the connection options for the integrated temperature sensor. Note that these options are set at the factory, based on the option ordered, and cannot be adjusted by the user.

For more information on configuring your analogs using the web interface, see the section titled, "Configuring Analogs" in the "Web Interface" section of this manual.

5.7 Discrete Alarms



Discrete alarm points can connect as a dry contact or a contact to ground

The NetGuardian 420 features up to 20 discrete alarm inputs - also called "digital inputs" or "contact closures". Discrete alarms are either active or inactive, so they're typically used to monitor on/off conditions like power outages, equipment failures, door alarms and so on.

The NetGuardian's discrete alarm points are single-lead signals referenced to ground. The ground side of each alarm point is internally wired to ground, so alarm points can connect either as a dry contact or a contact to ground.

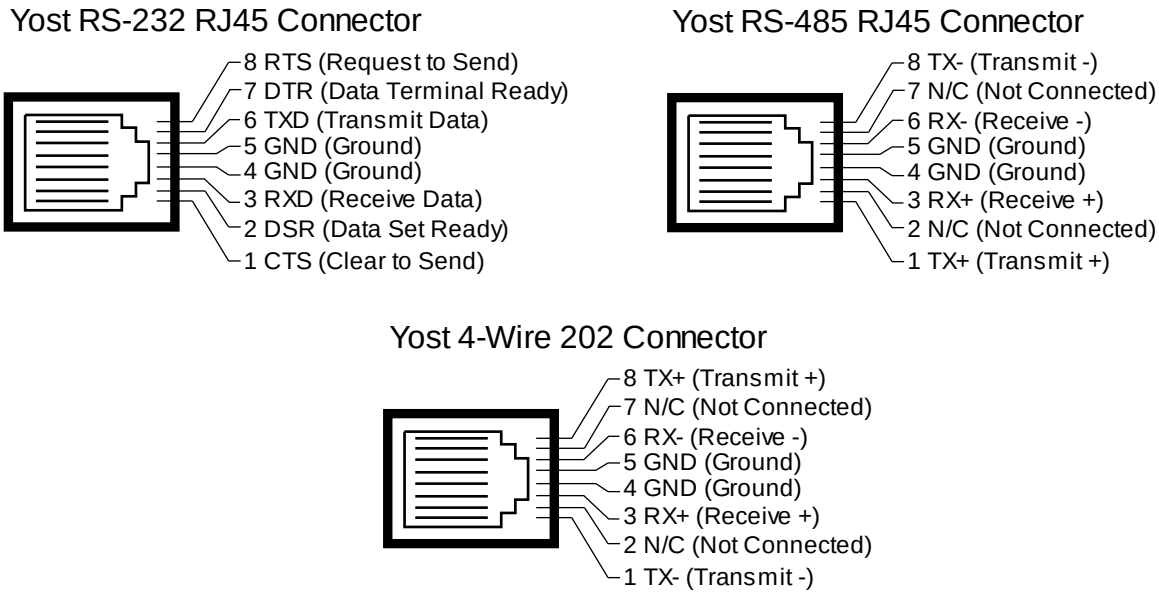
In a dry contact alarm: The alarm lead brings a contact to the ground lead, activating the alarm.

In a contact to ground alarm: A single wire brings a contact to an external ground, activating the alarm.

You can reverse the polarity of each individual discrete alarm point, so that the alarm is activated when the contact is open. This is done with a software configuration change.

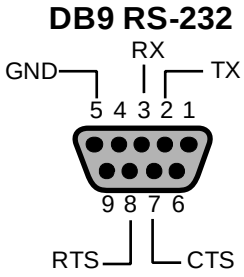
5.8 Data Ports

The NetGuardian's 4 terminal server ports provide reach-through terminal server functionality for connecting multiple simultaneous users to external equipment via Telnet over LAN. Each port can function as a proxy connection to an external device, a craft port, a channel port, a TCP or UDP reach-through port. The NetGuardian can support simultaneous proxy connections for up to 4 users.



Data port pinouts

NetGuardian data ports can be configured for Yost RS-232 or RS-485.These data ports are available as optional builds on NetGuardian hardware units (Call DPS Sales for more information @ 1-800-693-0351).



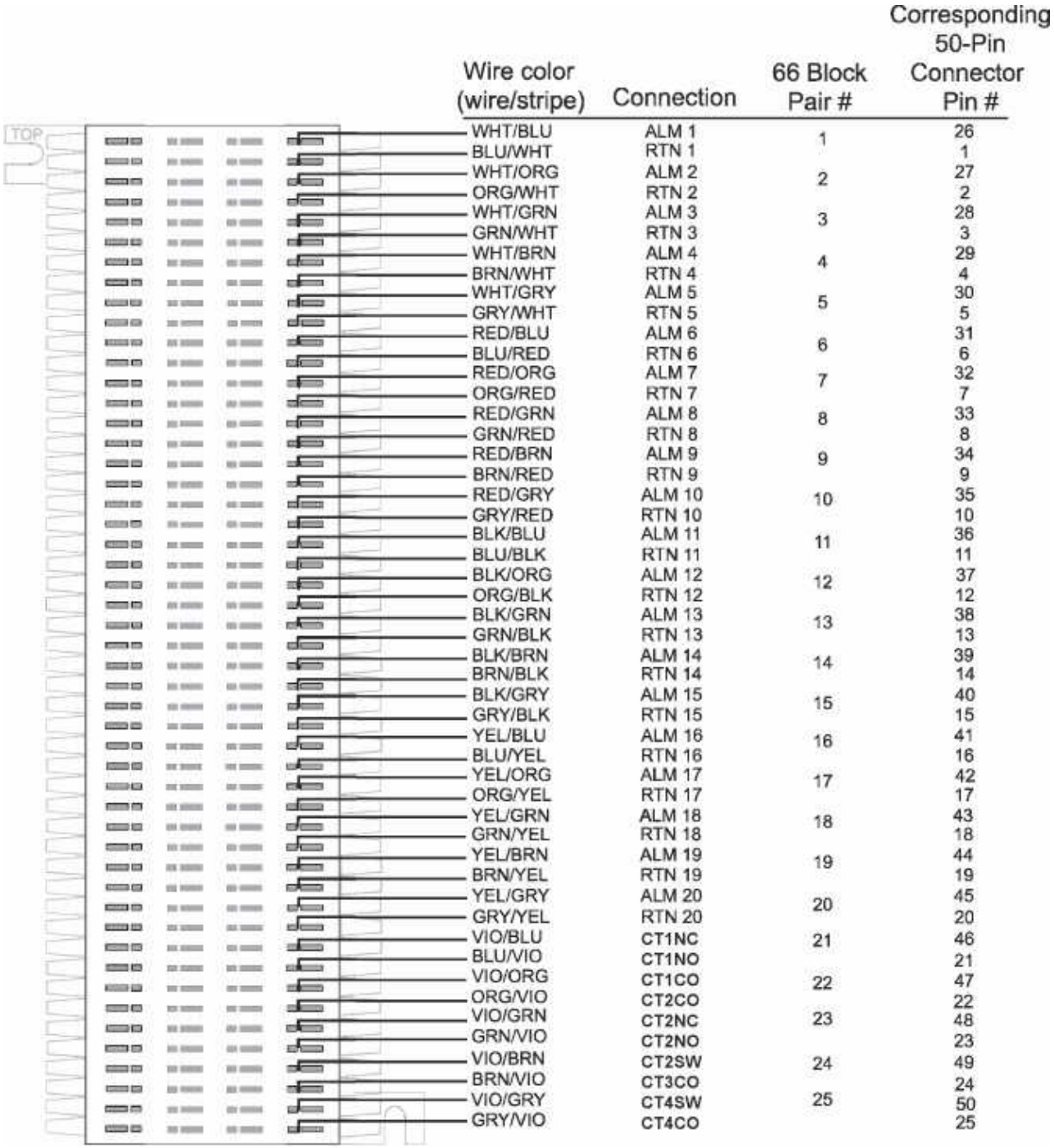
Pin #	Signal	Description
1		Not connected
2	**TX**	**Transmit data**
3	**RX**	**Recieve Data**
4		Not connected
5	**GND**	**Ground**
6		Not connected
7	**CTS**	**Clear to send**
8	**RTS**	**Request to send**
9		Not connected

*DB9 RS-232 Pinouts (**Craft Port Only**)*

5.9 Optional 66 Block Connector

The 50-pin connectors on the back panel of the NetGuardian can be connected to the optional 25-pair 66 Block Connector (part number D-PR-966-10A-00).

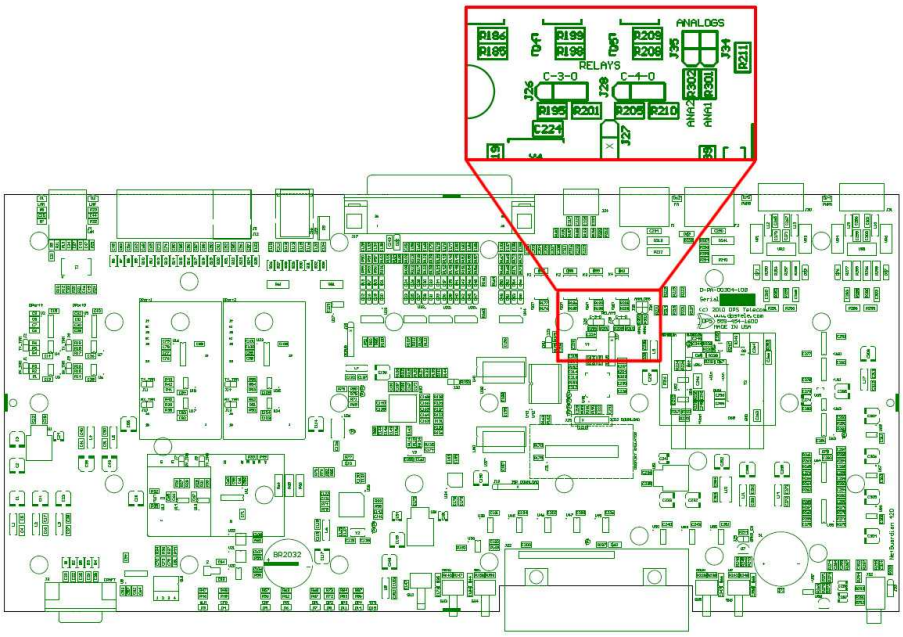
Note: If connecting to a 50-pair split block, all connections should be made on the two pin columns closest to the right-hand side of the block or bridge clips should be installed.



Wire color (wire/stripe)	Connection	66 Block Pair #	Corresponding 50-Pin Connector Pin #
WHT/BLU	ALM 1	1	26
BLU/WHT	RTN 1		1
WHT/ORG	ALM 2	2	27
ORG/WHT	RTN 2		2
WHT/GRN	ALM 3	3	28
GRN/WHT	RTN 3		3
WHT/BRN	ALM 4	4	29
BRN/WHT	RTN 4		4
WHT/GRY	ALM 5	5	30
GRY/WHT	RTN 5		5
RED/BLU	ALM 6	6	31
BLU/RED	RTN 6		6
RED/ORG	ALM 7	7	32
ORG/RED	RTN 7		7
RED/GRN	ALM 8	8	33
GRN/RED	RTN 8		8
RED/BRN	ALM 9	9	34
BRN/RED	RTN 9		9
RED/GRY	ALM 10	10	35
GRY/RED	RTN 10		10
BLK/BLU	ALM 11	11	36
BLU/BLK	RTN 11		11
BLK/ORG	ALM 12	12	37
ORG/BLK	RTN 12		12
BLK/GRN	ALM 13	13	38
GRN/BLK	RTN 13		13
BLK/BRN	ALM 14	14	39
BRN/BLK	RTN 14		14
BLK/GRY	ALM 15	15	40
GRY/BLK	RTN 15		15
YEL/BLU	ALM 16	16	41
BLU/YEL	RTN 16		16
YEL/ORG	ALM 17	17	42
ORG/YEL	RTN 17		17
YEL/GRN	ALM 18	18	43
GRN/YEL	RTN 18		18
YEL/BRN	ALM 19	19	44
BRN/YEL	RTN 19		19
YEL/GRY	ALM 20	20	45
GRY/YEL	RTN 20		20
VIO/BLU	CT1NC	21	46
BLU/VIO	CT1NO		21
VIO/ORG	CT1CO	22	47
ORG/VIO	CT2CO		22
VIO/GRN	CT2NC	23	48
GRN/VIO	CT2NO		23
VIO/BRN	CT2SW	24	49
BRN/VIO	CT3CO		24
VIO/GRY	CT4SW	25	50
GRY/VIO	CT4CO		25

Optional 66 block pinout for Discretes 1–20

5.10 Controls



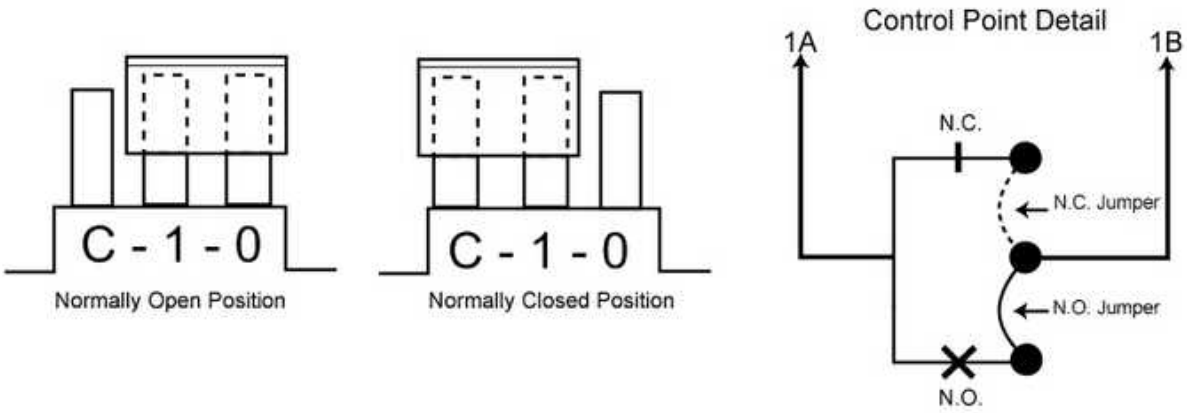
Adjustable jumpers on the NetGuardian 16A circuit board

Control Relays 3 and 4 on your NetGuardian are configured for Normally Open or Normally Closed (NO/NC) operation via jumpers on the NetGuardian's PC board.

By default, relays 3 and 4 are set for Normally Open (NO) operation.

To access your control relay jumpers, remove the top of the NetGuardian chassis. Start by removing the top 3 screws on the unit, then the bottom 3 screws. Remove the front 2 screws on the craft port and remove the lid.

WARNING: Always observe anti-static precautions whenever accessing your NetGuardian's PC Board



Jumper settings for analog alarm inputs and control relays

Reference the jumper settings in the image above to correctly configure Control Relays 3 and 4.

Note: Default control relay operation may differ depending on your NetGuardian's build options.

6 LCD Display

NetGuardian Front Panel LCD

The front panel LCD displays the current alarm and control status and provides a command menu for controlling the NetGuardian's basic functions.

Using the LCD command menu
The four buttons surrounding the front panel LCD are used to access the LCD Command Menu. To access the menu, press the Menu button. To scroll the menu, use the ▼ and ▲ buttons. To select a menu command, press the Sel (Select) button.

Standard Prompt
When no Command Menu item is selected and no alarms or relays are active, the LCD displays the firmware version and the standard prompt, `Press MENU for front panel options.`

Controlling Display Speed
The scroll speed can be temporarily increased by pressing and holding the ▲ button while the message is active.

6.1 Alarm and Control Status Messages

If an alarm or control relay is active, the LCD will display the following messages to indicate alarm and control status. The LCD panel will display the following messages to indicate alarm and control status:

Discrete Alarms:	If there are any standing discrete alarms, the display will read "Discrete Alarms:", followed by the user-defined descriptions of the standing alarm points.
Relays:	If there are any latched relays, the display will read "Relays:", followed by the user-defined descriptions of the latched relays.
Ping Alarms:	If any ping targets have failed to respond within the specified time, the display will read "Ping Alarms:", followed by the user-defined descriptions of the ping targets.
Analogs:	If any analog channels have crossed a threshold value, the display will read "Analogs", followed by the user-defined description of the analog channel, the channel's last voltage reading, and a letter indicating which threshold the channel has crossed.

Analog thresholds are represented by the following characters:
Major Over: a capital **O**
Minor Over: a lower-case **o**
Minor Under: a lower-case **u**
Major Under: a capital **U**

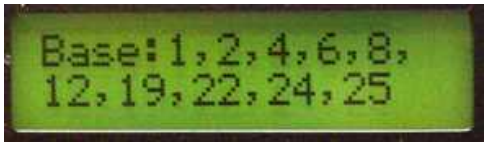
New LCD Function - "Point Mode"
This new feature allows you to change the way active alarms are displayed on the NetGuardian's front panel LCD screen. When the LCD is in "Point Mode," only the display points in alarm are displayed on the screen, instead of the full alarm descriptions. Point numbers for discrete alarms, analog threshold crossings, and latched relays will appear on the LCD. "Point Mode" is configurable from the TTY command line interface or the Web Interface

The following windows are supported and are processed in this order:

1. Base Alarms
2. Expansion 1 Alarms
3. Expansion 2 Alarms
4. Expansion 3 Alarms
5. Ping Alarms
6. Base Relays
7. Expansion 1 Relays
8. Expansion 2 Relays
9. Expansion 3 Relays
10. Base Analogs
11. Expansion 1 Analogs
12. Expansion 2 Analogs
13. Expansion 3 Analogs
14. Network Link Down

Only windows with alarms will appear on the LCD. If no alarms are active, a "no alarms active" message will appear. The LCD Delay Time is how long you want the points to show on the screen. You can set the delay time from 1-60 sec (default is 2 sec.) This is configurable from the TTY command line interface or the web interface.

Using the Front Panel LCD buttons for Point Mode
Pressing the SEL, ▲, or ▼ buttons will force the NetGuardian back into Scroll Mode for 3 minutes. This is particularly useful for viewing the configured descriptions or analog values associated with the active alarms. When Point Mode is enabled, but you chose to go into Scroll Mode, press the MENU button twice to go back.



See section "New! TTY Command Mode" for instructions on enabling / disabling Point Mode.

6.2 LCD Command Menu

LCD display

The LCD Command Menu provides commands for controlling some of the NetGuardian's basic functions: temporarily silencing the alarm speaker, rebooting the unit, and running the TTY configuration utility.

When no Command Menu item is selected and no alarms or relays are active, the LCD displays the firmware version and the Standard Prompt, `Press MENU for front panel options.` (See Figure 7.3.1, above.) To access the Command Menu, press the Menu button.

6.2.1 Sound off

Sound Off command

Sound off
The Sound off command suppresses sounds from the alarm speaker for a user-defined period of 10, 20, or 30 minutes. **To scroll to the next menu command,** press the ▼ button.

To change the Sound off setting, press Sel to select the command. The arrow cursor (>) will move to the right of the colon (:) in **Sound off:** to indicate that the command submenu is selected. Press the ▼ and ▲ buttons to scroll through the Sound off time period options. Select 0 minutes to allow all sounds. When the time period you want is displayed, press Sel to make your selection. **To exit the Command Menu** without changing the Sound off setting, press Menu.

6.2.2 Reboot

Reboot command

Reboot
The Reboot command reboots the NetGuardian. Press Sel. The LCD will briefly display the message `Rebooting ...`, and the normal boot sequence will begin. **To exit the Command Menu** without rebooting, press Menu.

6.2.3 Run Config

Run Config command

Run Config
The Run Config command forces the TTY configuration interface to run over the craft port at the user defined baud rate (default is 9600 baud).

To run the TTY configuration utility, press Sel. **To exit the Command Menu** without running the TTY interface, press Menu.

6.2.4 Contrast

Contrast command

Contrast
The **Contrast** command provides controls for adjusting the contrast of the LCD.

To adjust the contrast, press Sel to select the command. The arrow cursor (>) will move to the right of the

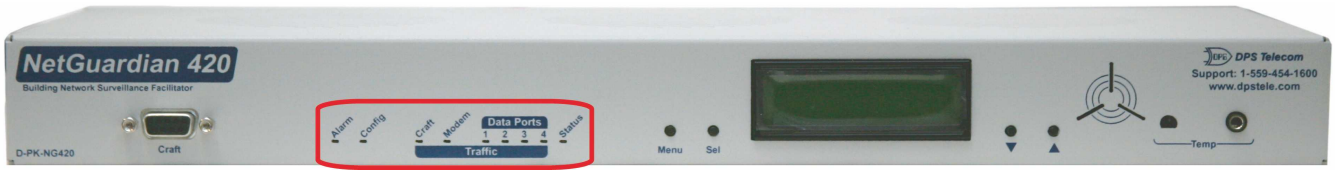
colon (:) in `Contrast:` to indicate that the command submenu is selected. Press the ▼ or ▲ button until you're satisfied with the contrast setting, then press Sel to make your selection. **To exit** the Command Menu and **revert to the default contrast setting**, press Menu.

7 Alarm Speaker

The NetGuardian's alarm speaker emits distinctive tones under two conditions

1. **If there is an Ethernet connection failure,** the speaker will emit a intermittent beep**.** Press any front panel button to silence the speaker.
2. **If an alarm occurs,** the speaker will emit an **intermittent beep**. Press any front panel button to silence the speaker. If you do not silence the speaker, the beep will continue for the user defined duration (default is a 6 second duration). Silencing the speaker will allow the next alarm, if any, to sound.

8 Front Panel LEDs



Front panel LEDs

The NetGuardian's front panel LEDs indicate communication and alarm reporting status. LED status messages are described below.

LED	Status	Description
Config	Blink Green	Valid Configuration
	Blink Red	Invalid Configuration
Alarm	Blink Red	New COS alarm*
	Solid Red	One or more standing alarms*
Craft	Blink Green	Transmit over craft port
	Blink Red	Receive over craft port
Modem	Blink Green	Transmit over Modem port
	Blink Red	Receive over Modem port
Data Ports1-4	Blink Green	Transmit over indicated data port
	Blink Red	Receive over indicated data port
Status	----	Reserved for future use of hardware accelerator.

***NOTE:** Alarm must be configured for notification to be reflected in LED

Front panel LED Status message descriptions

9 Back Panel LEDs

Back panel LEDs for Power (left) and Ethernet connections

The back panel LEDs indicate the status of power and Ethernet connections. LED status messages are described below in Table 10.A.

LED	Status	Description
Power A and/or B	Solid Green	Polarity is correct on power feed A or B.
	Off	No Power or Polarity Reverse
FA	Solid Red	Fuse failure
Net1	Blink Green	Activity over indicated integrated Ethernet port

Back panel LED Status message descriptions

10 Configuring the NetGuardian

The NetGuardian must be provisioned with log-on passwords, alarm descriptions, port parameters, ping targets, control descriptions, and other system information. Most provisioning will be done via the NetGuardian Web Interface. The NetGuardian also supports a limited TTY interface (used mostly for initial unit configuration.)

You can provision the NetGuardian IP Address either locally through the craft port or remotely through a LAN connection. However, to access the NetGuardian via LAN you must first make a temporary connection to the NetGuardian and assign it an IP address on your network. For more information, see the following section, "Connecting to the NetGuardian."

10.1 RADIUS Authentication

RADIUS authentication is now supported by any NetGuardian 420 platform.

RADIUS (Remote Authentication Dial In User Service) is an industry-standard way to manage logins to many different types of equipment in one central location. The NetGuardian connects to your central RADIUS server. Every time a device receives a login attempt (usually a username & password), it requests an authentication from the RADIUS server. If the username & password combination is found in the server's database, an affirmative "access granted" reply is sent back to the unit device, allowing the user to connect.

Also included in the reply are the user's individual access rights, so different users can be granted different privilege levels. If the user's login attempt is not found, a rejection is returned instead. RADIUS configuration for the NetGuardian will be achieved via the web browser interface or TTY interface. For details, see the separate user manuals for the NetGuardian 420 web browser.

11 Connecting to the NetGuardian

11.1 ... via Craft Port

NetGuardian Craft Port

The simplest way to connect to the NetGuardian is over a physical cable connection between your PC's COM port and the NetGuardian's craft port.

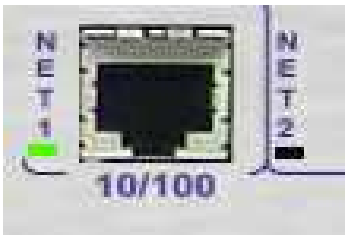
Use the DB9M-DB9F download cable provided with your NetGuardian to make a craft port connection.

Select the following COM port options:
• Bits per second: **9600**
• Data bits: **8**
• Parity: **None**
• Stop bits: **1**
• Flow control: **None**

The default password is 'dpstelecom'

You can perform basic configuration via the craft port - but if you like, you can connect via the craft port just to configure the NetGuardian's Private LAN IP address, and then do the rest of your configuration via a LAN connection.

11.2 ... via LAN



Ethernet port 1

You can also connect to the NetGuardian over a LAN connection. This is a very convenient way to provision multiple NetGuardian units at multiple locations.

To connect to the NetGuardian via LAN, all you need is the unit's IP address (Default IP address is 192.168.1.100).

Note: NET is defaulted to 192.168.1.100

If you have physical access to the NetGuardian, the easiest thing to do is connect to the unit through the craft port and then assign it an IP address. Then you can complete the rest of the unit configuration over a remote LAN connection, if you want. For instructions, see Section 12.1, "Connecting to the NetGuardian via Craft Port."

If you DON'T have physical access to the NetGuardian, you can make a LAN connection to the unit by temporarily changing your PC's IP address and subnet mask to match the NetGuardian's factory default IP settings. Follow these steps:

1. Look up your PC's current IP address and subnet mask, and write this information down.

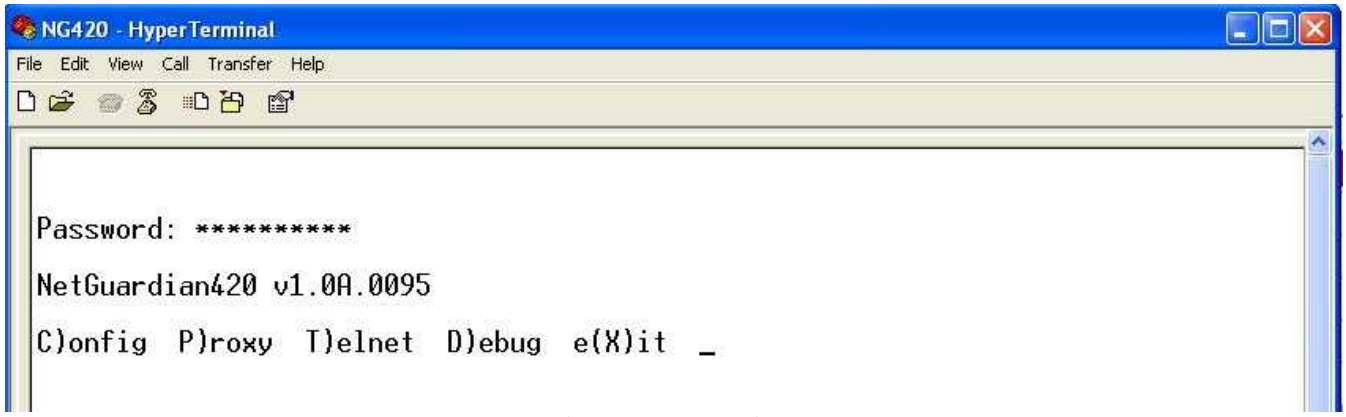
2. Reset your PC's IP address to **192.168.1.200**.

3. Reset your PC's subnet mask to **255.255.0.0**. You may have to reboot your PC to apply your changes.

4. Once the IP address and subnet mask of your computer coincide with the NetGuardian's, you can access the NetGuardian via a Telnet session or via Web browser by using the NetGuardian's default IP address of **192.168.1.100**.

5. Provision the NetGuardian with the appropriate information, then change your computer's IP address and subnet mask back to their original settings.

12 TTY Interface



The TTY interface initial configuration screen

The TTY interface is the NetGuardian's built-in provision controls for basic configuration of the NetGuardian. Configure the NetGuardian's ethernet port settings, monitor the status of base and system alarms, operate control relays, view live ping targets , view debug or create proxy connections to other ports.

To use the TTY interface with the NetGuardian, all you need is any PC with terminal emulation software (i.e. Hyperterminal) and a connection to the NetGuardian. This connection can be a direct connection to the NetGuardian's front panel craft port or a remote connection via Telnet or dial-up

Some initial software configuration must be performed before you can use a remote connection to the NetGuardian. For Telnet, connect to the Net Guardian's IP address at port 2002 to access the configuration menus after initial LAN/WAN setup. **Telnet sessions are established at port 2002, not the standard Telnet port** as an added security measure.

The TTY interface is primarily used for configuring and provisioning the NetGuardian, but you can also use it to ping IP targets, view system statistics, and data port activity.

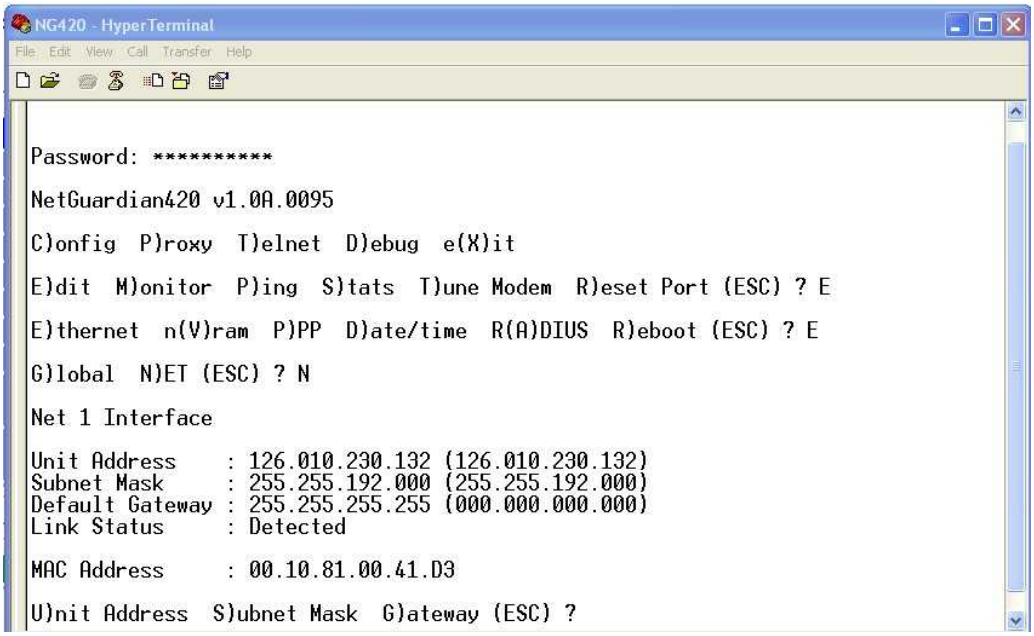
NOTE: The TTY default password is "dpstelecom".

Menu Shortcut Keys
The letters before or enclosed in parentheses ( ) are menu shortcut keys. Press the shortcut key to access that option. Pressing the ESC key will always bring you back to the previous level. Entries are not case sensitive.

12.1 Unit Configuration

12.1.1 Ethernet Port Setup

The NetGuardian must be assigned an IP address before you will be able to connect via LAN/WAN using a Telnet client or a Web browser. To connect via LAN, the minimum configuration requires setup of the IP address and subnet mask. Minimum WAN configuration requires that the default gateway be set as well. Follow the instructions below to configure the NetGuardian's IP address, subnet mask, default gateway, trap address, SNMP port number, proxy base, and DHCP option.


NG420 - HyperTerminal
File Edit View Call Transfer Help
Password: **********
NetGuardian420 v1.0A.0095
C)onfig P)roxy T)elnet D)ebug e(X)it
E)dit M)onitor P)ing S)tats T)une Modem R)eset Port (ESC) ? E
E)thernet n(V)ram P)PP D)ate/time R(A)DIUS R)eboot (ESC) ? E
G)lobal N)ET (ESC) ? N
Net 1 Interface
Unit Address : 126.010.230.132 (126.010.230.132)
Subnet Mask : 255.255.192.000 (255.255.192.000)
Default Gateway : 255.255.255.255 (000.000.000.000)
Link Status : Detected
MAC Address : 00.10.81.00.41.D3
U)nit Address S)ubnet Mask G)ateway (ESC) ?

Configure the Ethernet port parameters

1. Connect using Hyperterminal @ 9600, 8, N, 1.

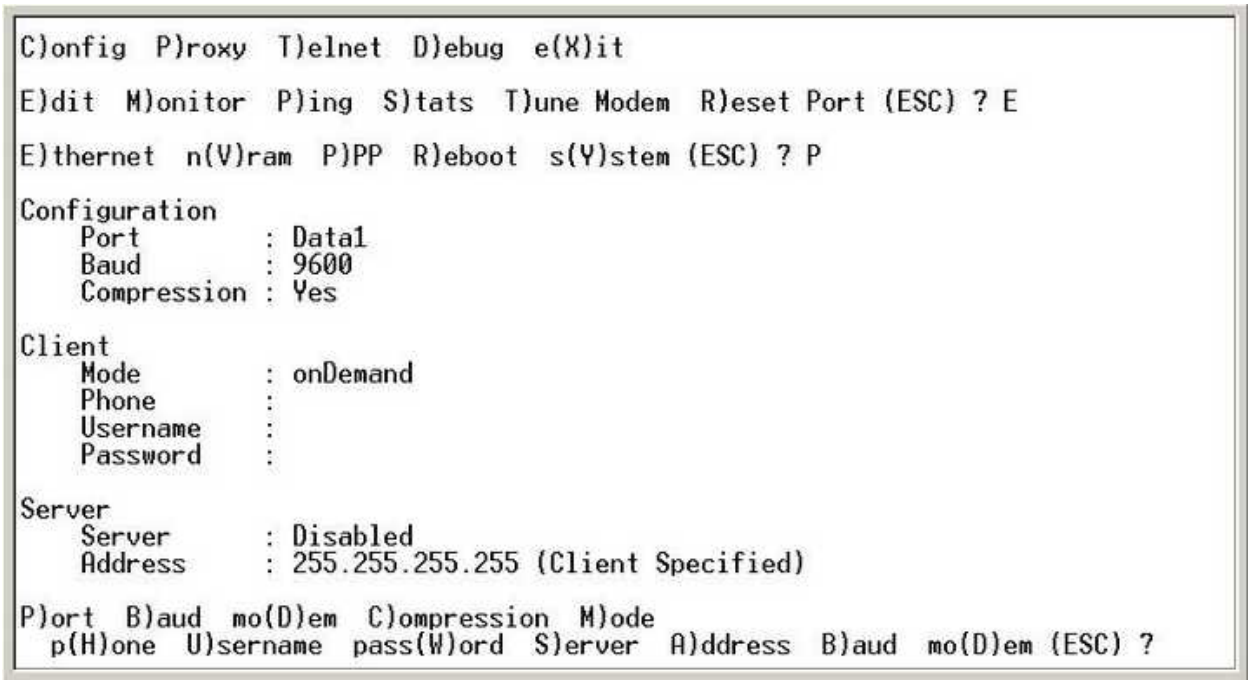
2. Hit enter (you won't be able to see this text), the NetGuardian will respond with "Password."
   Note: If you receive no password prompt then check the port you are using on your PC and make sure you are using a straight thru cable.
3. Type the default password, "dpstelecom," then press Enter.
   Note: DPS strongly recommends changing the default password.
4. The NetGuardian's main menu will appear.
5. Type C for the C)onfig menu.
6. Type E for E)dit menu.
7. Type E for port settings, N for Net.
8. Configure the unit address, subnet mask, and default gateway.
9. ESC to the main menu.
10. When asked if you would like to save changes, type Y (yes).

11. Reboot to save the new configuration to the NetGuardian.
12. Now you can connect to the NetGuardian via LAN and use the Web Browser Interface to complete the configuration.

⚠ RADIUS logons **are** case-sensitive. If the RADIUS server is unavailable or access is denied, the master password will work for craft port access only. Also, the "dictionary.dps" files (included on the Resource Disk) needs to be loaded on the RADIUS server for access-right definition. If RADIUS is enabled on the NetGuardian, local authentication will not be valid.

12.1.2 Edit PPP Port

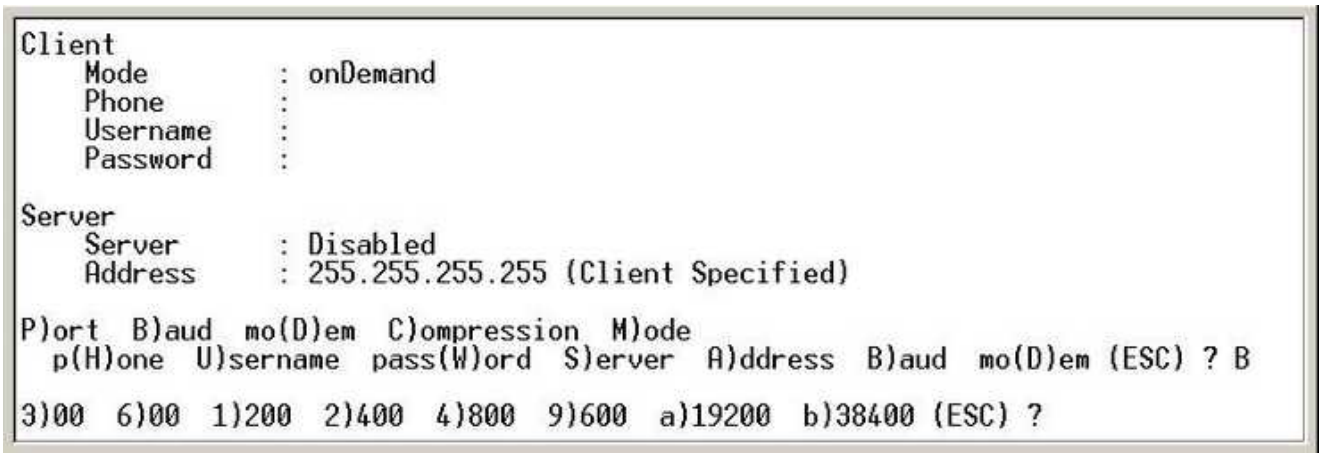
Choose P)PP to edit your baud rate, depending on what device has been chose for the PPP port.



Edit your PPP port

If you are using a modem for the PPP port, then choose mo(D)emto define the modem initialization strings.

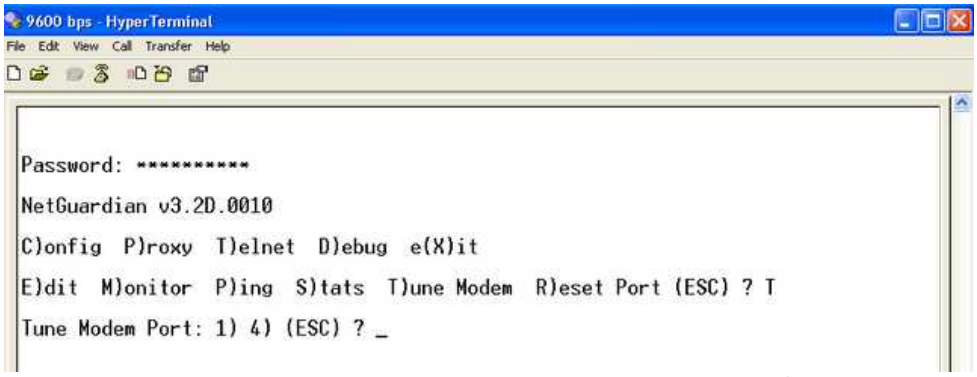
Choose B)aud to define the baud rate for that port.


Client
Mode : onDemand
Phone :
Username :
Password :
Server
Server : Disabled
Address : 255.255.255.255 (Client Specified)
P)ort B)aud mo(D)em C)ompression M)ode
p(H)one U)sername pass(W)ord S)erver A)ddress B)aud mo(D)em (ESC) ? B
3)00 6)00 1)200 2)400 4)800 9)600 a)19200 b)38400 (ESC) ?

Select the baud rate for your PPP port

12.1.3 Tune 202 Modem

Tuning the 202 modem on a NetGuardian 420 can only be done from the TTY interface (using either HyperTerminal through the front craft port or by telnet over LAN on port 2002).


9600 bps - HyperTerminal
File Edit View Call Transfer Help
Password: **********
NetGuardian v3.2D.0010
C)onfig P)roxy T)elnet D)ebug e(X)it
E)dit M)onitor P)ing S)tats T)une Modem R)eset Port (ESC) ? T
Tune Modem Port: 1) 4) (ESC) ? _

Press 'T' to tune the 202 Modem with the TTY interface

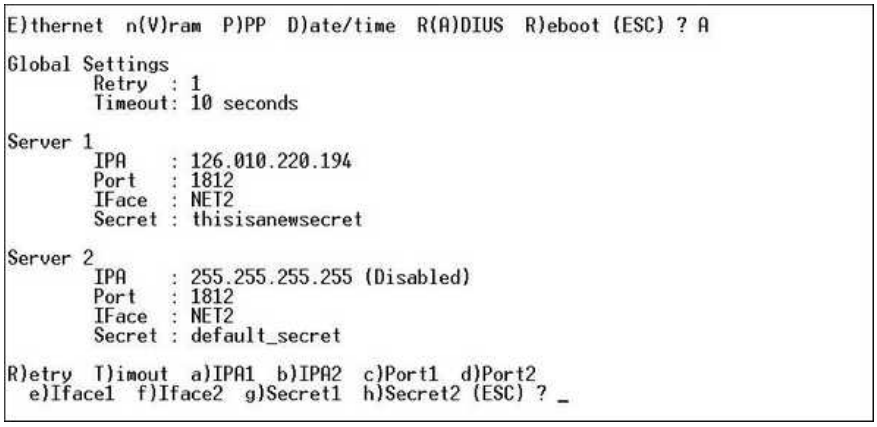
Though no menu options will appear, use the following commands to tune the 202 modem. Each menu option, when chosen, will output the character "A" on screen:

1) Minor Adjust DB+
2) Minor Adjust DB-
3) High Frequency
4) Low Frequency
5) Off
6) Major Adjust DB-
7) Major Adjust DB+
8) Median Frequency (Average of high and low frequency)

After selecting an option (like #1 in this example) for Minor Adjust the DB+ level, the NetGuardian will return a '+' command to inform you the task is completed. Each time you hit a number key (1-8), the NetGuardian will a '+' on your screen.

12.1.4 RADIUS Configuration

The TTY interface can also be used to configure RADIUS settings. After entering the IPA for the RADIUS server, users will be prompted for both a username **and** password to logon to the unit. This username and password combination will be verified against the RADIUS database, and not the local database. The local password database will only be used for front panel craft port access in the event the RADIUS configuration is making the unit otherwise inaccessible.



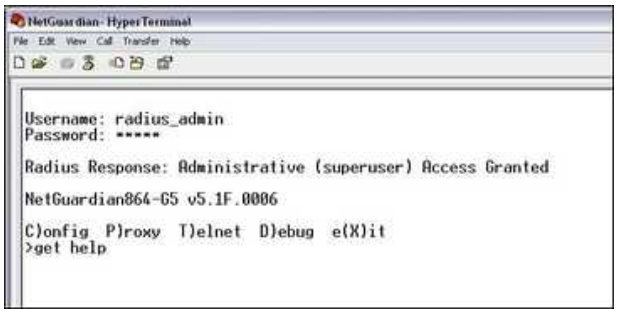
The RADIUS configuration menu using the TTY interface.

Global Settings	
Retry	How many times the RADIUS server will retry a logon attempt
Time-out	Enter in the number of seconds before a logon request is timed out
Servers 1 / 2	
IPA	Enter the IP address of the RADIUS server
Port	Port 1812 is an industry-standard port for using RADIUS
Interface	Use the drop-down menu to choose NET1.
Secret	Enter the RADIUS secret in this field

RADIUS logon screen prompts for a Username and Password.

12.1.5 New! - TTY Command Mode

This command line mode offers an alternate way of configuring the NetGuardian 420. This interface is scriptable, and is recommended for advanced users. Entries are NOT case sensitive.



To enter Command Line mode, login to the TTY, then press Ctrl+C.

Tips for using TTY Command Mode

- To enter command mode, login to the TTY interface and press Ctrl + C.
- To view all acceptable operations, type **get help**, then press Enter.
- Invalid commands will return "Error" as the response.
- A **CRLF** is sent by the RTU following all responses from the RTU.
- When setting commands, be sure to use "=" between the command and its parameter.
- See the examples later in this section for more help with TTY mode.

- Limited data validation is in place using this method. Use caution when setting variable values.
- In some cases, you need to reboot the NetGuardian for new variable values to take effect.
- Changing **REF1**, **REF2**, **DISP1**, or **DISP2** affects the **MAJOR, MINOR, OVER**, and **UNDER** alarm thresholds. Changing any of these settings should be checked and re-established as required.
- In the table below, variables (params) are noted in brackets.

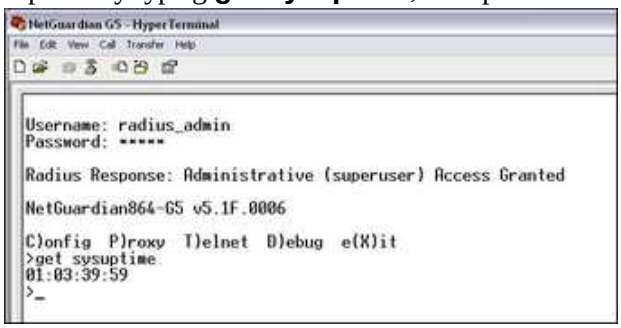
Operation	Command	Params
Help	get help	None
Initialize NVRAM	init nvram {g2}	None
Write NVRAM	set nvram	None
Read NVRAM	get nvram	None
View System Up Time	get sysuptime	None
View Firmware Version	get prodid	None
Data Port Description	{get,set} dataport {1...4} desc	string {0...15} chars
Data Port Baud	{get,set} dataport {1...4} baud	{1200,300,600,1200,2400,4800, 9600,19200,38400,57600,115200 }
Data Port Format	{get,set} dataport {1...4} wfmt	{8n1,8n2,7n1,7e1,7o1,8 o2,8o1}
Data Port RTS Head (msec)	{get,set} dataport {1...4} rtshead	{0..255}
Data Port RTS Tail (msec)	{get,set} dataport {1...4} rtstail	{0..255}
Data Port Type	{get,set} dataport {1...4} type	{off,tcp,ptcp,htcp,rtcp,udp,chan, crft,cap,ecu,sps8}
# of NetGuardian Expanders	{get,set} ngddx	{0...3}
# of GLD or BSU	{get,set} gld	{0...16}
Timed Tick Period	{get,set} timed tick	{0...60} {min}
System Name	{get,set} name	string {0..31} chars
System Location	{get,set} location	string {0..31} chars

System Contact	{get,set} contact	string {0..31} chars
System Phone	{get,set} phone	string {0..20} chars
Reboot	set reboot	None
DCP Unit ID	{get,set} dcpaddr	{0...255}
DCP Port Number	{get,set} dcpport	{1..32767}
DCP Port Type	{get,set} dcptype	{udp,tcp,serial}
DCP Protocol	{get,set} dcpprot	{dcpx,dcpf,dcpe}
DCP Autonomous Time	{get,set} dcpautotm	{0..120} {sec,min}
Network Time IPA	{get,set} ntpipa	IP Address
Username	{get,set} username {1...16}	string {0...18} chars
Password	set password {master, 1...16}	string {0..15} chars
Access Rights	{get,set} access {1...16}	{0000..01ff} where Bit.0 – 1=admin Bit.1 – 1=database Bit.2 – 1=monitor Bit.3 – 1=rly control Bit.4 – 1=reachthru Bit.5 – 1=modem Bit.6 – 1=telnet Bit.7 – 1=sd_monitor Bit.8 – 1=ppp
Network IPA	{get,set} net 1 ipa	IP Address
Subnet Mask	{get,set} net 1 subnet	Subnet
Gateway IPA	{get,set} net 1 gateway	Gateway
Proxy Base	{get,set} proxybase	{1..32767}
Analog Description	{get,set} alg {1...8} desc	string {0..48} chars
Analog Display Unit	{get,set} alg {1...8} unit	string {0..3} chars
Analog Major Under Threshold	{get,set} alg {1...8} thres mju	{-94.0000...94.0000}
Analog Minor Under Threshold	{get,set} alg {1...8} thres mnu	{-94.0000...94.0000}
Analog Minor Over Threshold	{get,set} alg {1...8} thres mno	{-94.0000...94.0000}
Analog Major Over Threshold	{get,set} alg {1...8} thres mjo	{-94.0000...94.0000}
Analog Trap	{get,set} alg {1...8} trap	0=trap disabled 1=trap enabled
Analog Primary Notification	{get,set} alg {1...8} pri	{0...8}
Analog Secondary Location	{get,set} alg {1...8} sec	{0...8}
Analog Polarity	{get,set} alg {1...8} polarity	0=Normal 1=Reversed
Analog Group Number	{get,set} alg {1...8} group {mju,mnu, mno,mjo}	{1...8}
Analog Reference 1 VDC	{get,set} alg {1...8} ref1	Number
Analog Reference 1 Display	{get,set} alg {1...8} disp1	Number
Analog Reference 2 VDC	{get,set} alg {1...8} ref2	Number
Analog Reference 2	{get,set} alg {1...8} disp2	Number

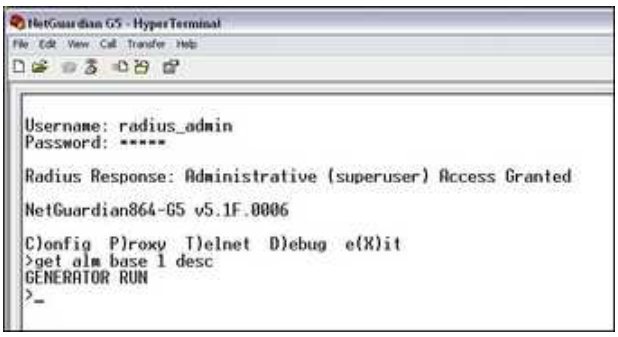
Display		
Analog Deadband	{get,set} alg {1...8} deadband	{0.1...9.9}
Alarm Description	{get,set} alm {base,exp1,exp2,exp3} {1...64} desc	string {0...48} chars
Alarm Polarity	{get,set} alm {base,exp1,exp2,exp3} {1...64} polarity	0=Normal 1=Reversed
Alarm Trap	{get,set} alm {base,exp1,exp2,exp3} {1...64} trap	0=trap disabled 1=trap enabled
Alarm Primary Notification	{get,set} alm {base,exp1,exp2,exp3} {1...64} pri	{0...8}
Alarm Secondary Notification	{get,set} alm {base,exp1,exp2,exp3} {1...64} sec	{0...8}
Alarm Group	{get,set} alm {base,exp1,exp2,exp3} {1...64} group	{1...8}
Global Trap IP Address	{get,set} trap {1,2} ipa	IP Address
Global Trap Format	{get,set} trap {1,2} format	{v1, v2c, v2cinf,v3}
LCD Display Mode	{get,set} lcdmode	{scroll,point}
LCD Delay Time (for Point Mode)	{get,set} lcddelay	{1..60} {sec}

Examples

- You want to find out how long this NetGuardian has been running (since last rebooted.) Get system uptime by typing **get sysuptime**, then press Enter.

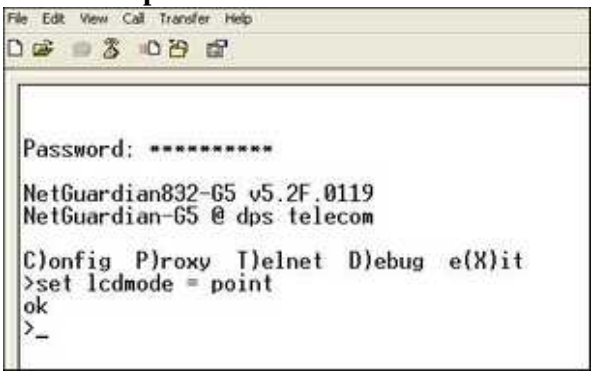


- You want to see the alarm description for Base Alarm 1. To see the description, type **get alm base 1 desc**



- You want to set the Global Trap IP Address to 126.10.230.133. To enter this, type **set trap 1 ipa = 126.10.230.133**

- You want to change the LCD mode from Scroll (default) to Point Mode. To change this, type **set lcdmode = point**



12.2 Monitoring

12.2.1 Monitoring the NetGuardian

Connect a PC running VT100 terminal emulation software to the craft port or connect via LAN using a Telnet client with VT100 emulation to port 2002 to reach the monitor menu selection. This section allows you to do full system monitoring of the NetGuardian including: all alarms, ping information, relays, analogs, and system status.

```
C)onfig  P)roxy  T)elnet  D)ebug  e(X)it

E)dit  M)onitor  P)ing  S)tats  T)une Modem  R)eset Port (ESC) ? M

A)larms  R)elays  a(N)alogs  E)vent log  a(C)cum. Timer
  B)AC  P)ing targets  p(O)rts  S)ystem (ESC) ?
```

The monitor menu allows status checking on all elements

12.2.1.1 Monitoring Base Alarms

View the status of the device connected to the discrete alarms from the M)onitor menu > A)larms option. Under **Status**, the word **Alarm** will appear if an alarm has been activated and **Clear** will appear if an alarm condition is not present. If groups are used the user defined status will be displayed.

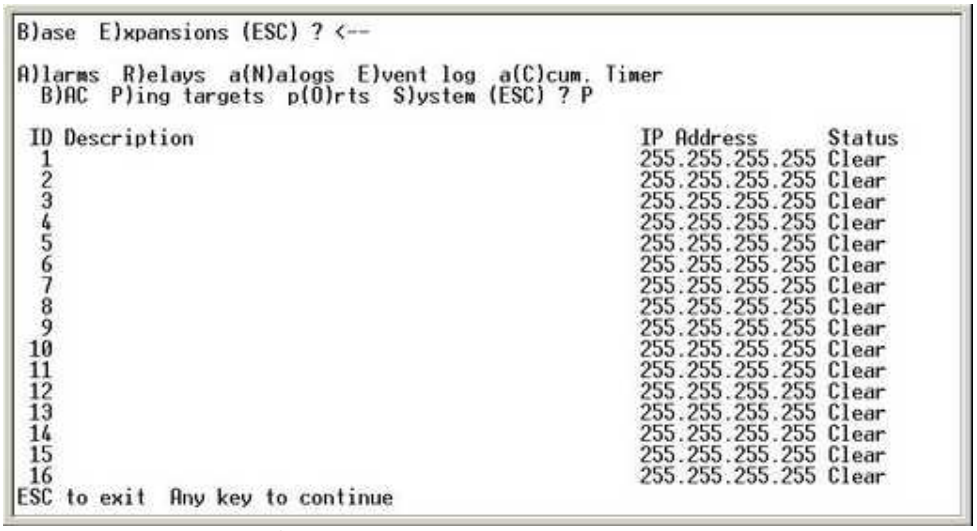
```
A)larms  R)elays  a(N)alogs  E)vent log  a(C)cum. Timer
  B)AC  P)ing targets  p(O)rts  S)ystem (ESC) ? A
B)ase  E)xpansions (ESC) ? B

 ID Description                                    Status
  1                                                Clear
  2                                                Clear
  3                                                Clear
  4                                                Clear
  5                                                Clear
  6                                                Clear
  7                                                Clear
  8                                                Clear
  9                                                Clear
 10                                                Clear
 11                                                Clear
 12                                                Clear
 13                                                Clear
 14                                                Clear
 15                                                Clear
 16                                                Clear
ESC to exit  Any key to continue
```

This example shows page two of the discrete alarms

12.2.1.2 Monitoring Ping Targets

View the status of all your ping targets from the M)onitor menu > P)ing targets option. This screen displays the ping target ID, description, and IP address. Under **Status** the word **Alarm** will appear if an alarm has been activated and **Clear** will appear if an alarm condition is not present.

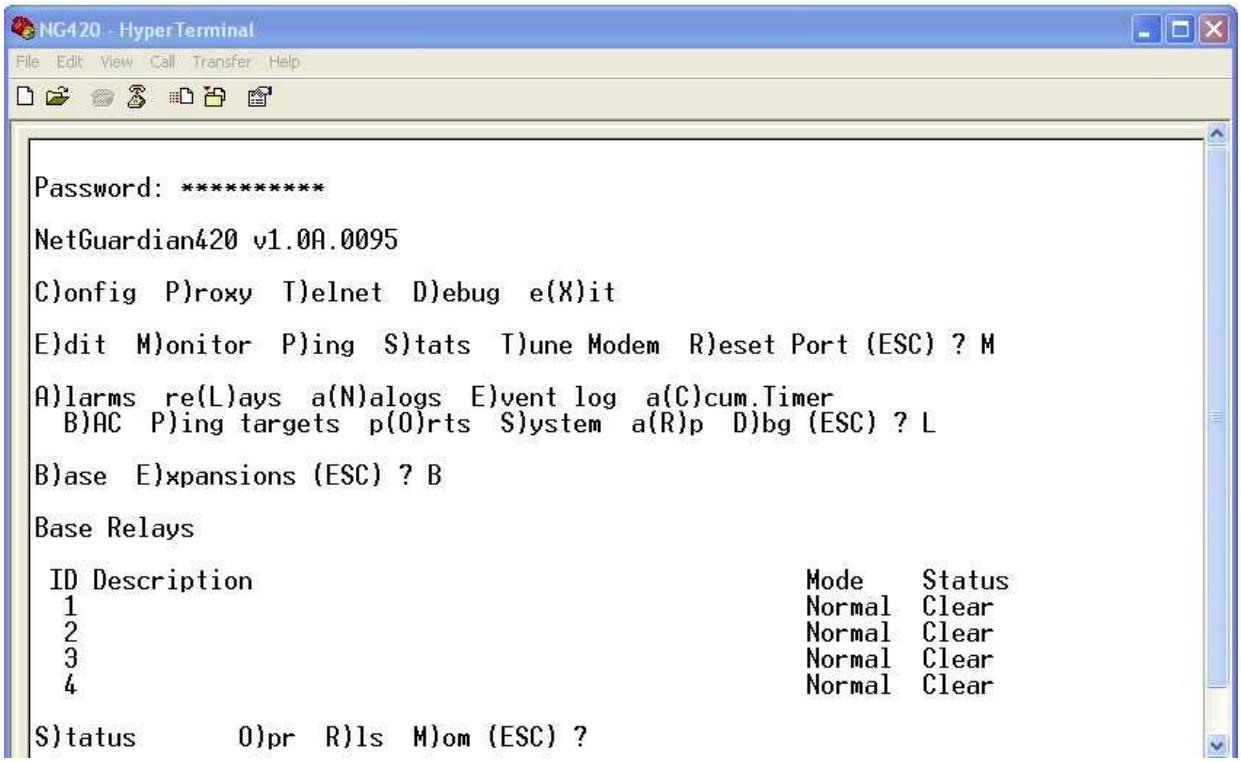


The Ping info submenu allows you to change ping targets

12.2.1.3 Monitoring and Operating Relays (Controls)

The NetGuardian comes equipped with 4 relays that can be used to control external devices. Monitor the status of your relays from the M)onitor menu > R)elays option.

Relays 3 and 4 are set to normally open (N/O) as the factory default, but each or all of them can be changed to normally closed (N/C) by changing their respective jumper.

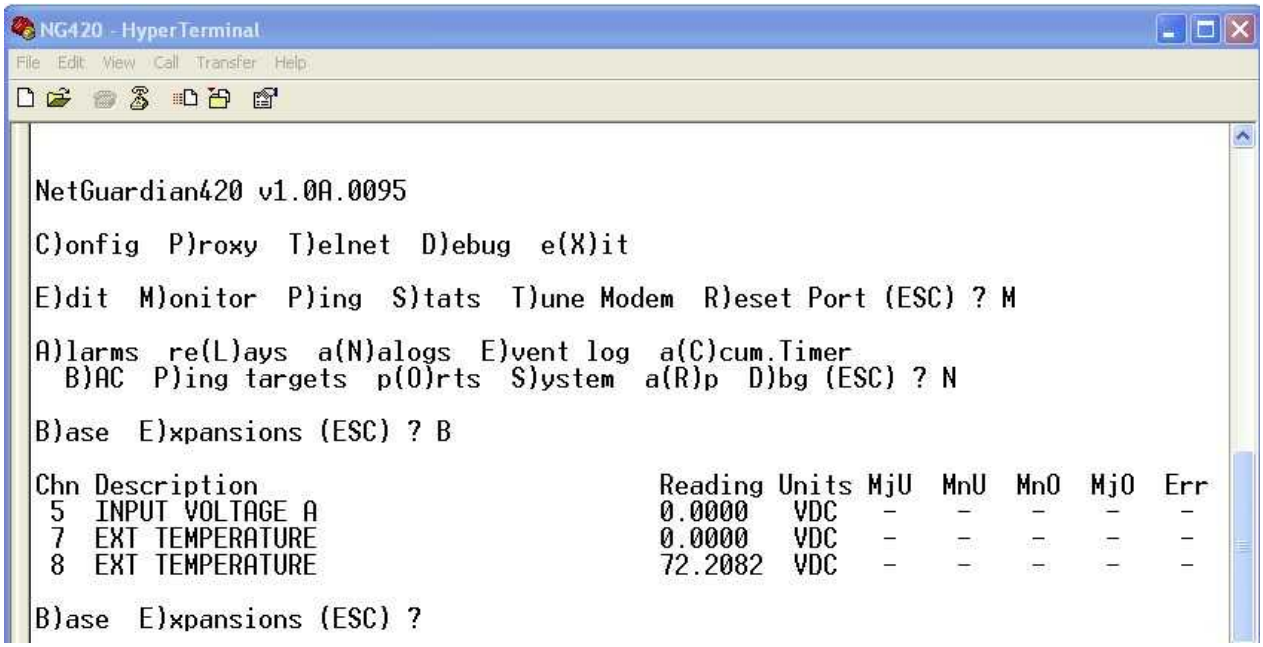

NG420 - HyperTerminal
File Edit View Call Transfer Help
Password: **********
NetGuardian420 v1.0A.0095
C)onfig P)roxy T)elnet D)ebug e(X)it
E)dit M)onitor P)ing S)tats T)une Modem R)eset Port (ESC) ? M
A)larms re(L)ays a(N)alogs E)vent log a(C)cum.Timer
B)AC P)ing targets p(O)rts S)ystem a(R)p D)bg (ESC) ? L
B)ase E)xpansions (ESC) ? B
Base Relays
ID Description Mode Status
1 Normal Clear
2 Normal Clear
3 Normal Clear
4 Normal Clear
S)tatus O)pr R)ls M)om (ESC) ?

The eight relays can be operated from this screen

12.2.1.4 Monitoring Analogs

View the current reading and the alarm status of your analog devices from the M)onitor menu > a(N)logs option. The value shown is a snapshot of the channels measurement, not a real-time reading. Refresh the readings by re-selecting the analogs option. Alarm status indicates that a preset threshold has been crossed and is designated by an **x**.

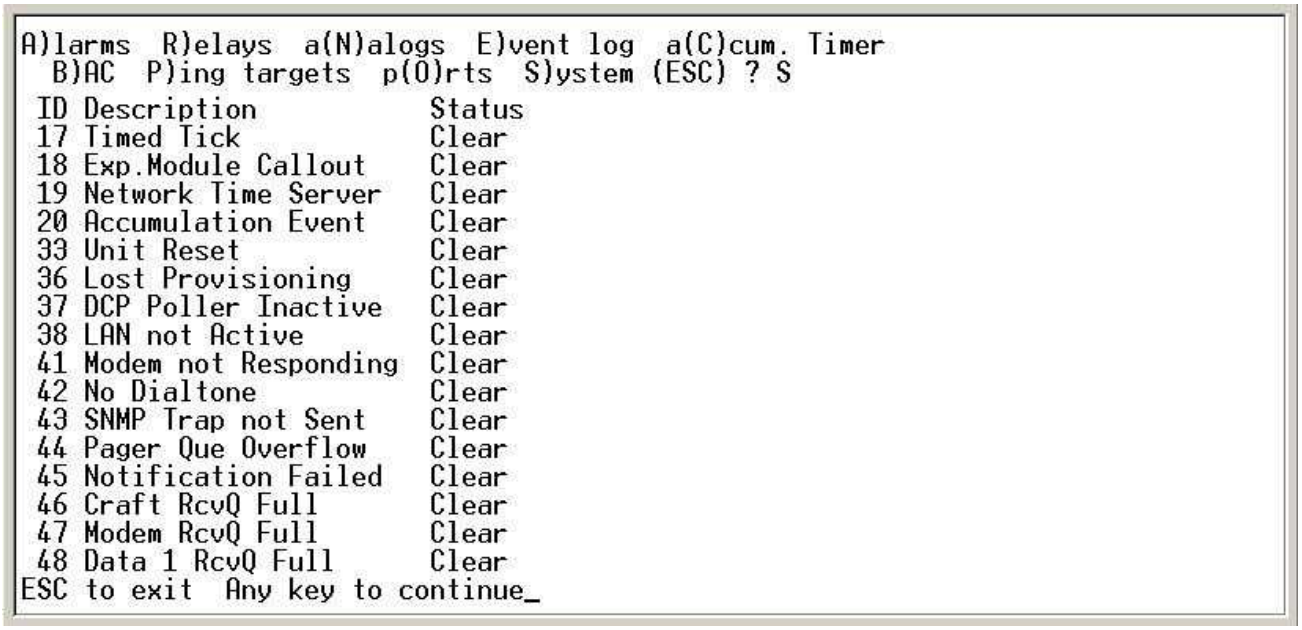
The 6 analog measuring inputs are set to measure voltage as the factory default. If your sensors output is current, change the appropriate analog shunt, to the current measuring position. The scaling worksheet in the provisioning section converts all readings shown here into native units, such as degrees Celsius or percent relative humidity.


NG420 - HyperTerminal
File Edit View Call Transfer Help
NetGuardian420 v1.0A.0095
C)onfig P)roxy T)elnet D)ebug e(X)it
E)dit M)onitor P)ing S)tats T)une Modem R)eset Port (ESC) ? M
A)larms re(L)ays a(N)alogs E)vent log a(C)cum.Timer
B)AC P)ing targets p(O)rts S)ystem a(R)p D)bg (ESC) ? N
B)ase E)xpansions (ESC) ? B
Chn Description Reading Units MjU MnU MnO MjO Err
5 INPUT VOLTAGE A 0.0000 VDC - - - - -
7 EXT TEMPERATURE 0.0000 VDC - - - - -
8 EXT TEMPERATURE 72.2082 VDC - - - - -
B)ase E)xpansions (ESC) ?

This display allows you to monitor your eight analog inputs

12.2.1.5 Monitoring System Alarms

View the status of the NetGuardian's system alarms from the M)onitor menu > S)ystem option. Under **Status**, the word **Alarm** will appear if an alarm has been activated and **Clear** will appear if an alarm condition is not present. See Appendix, "System Alarm Descriptions," for more information. If groups are used the user defined status will be displayed.

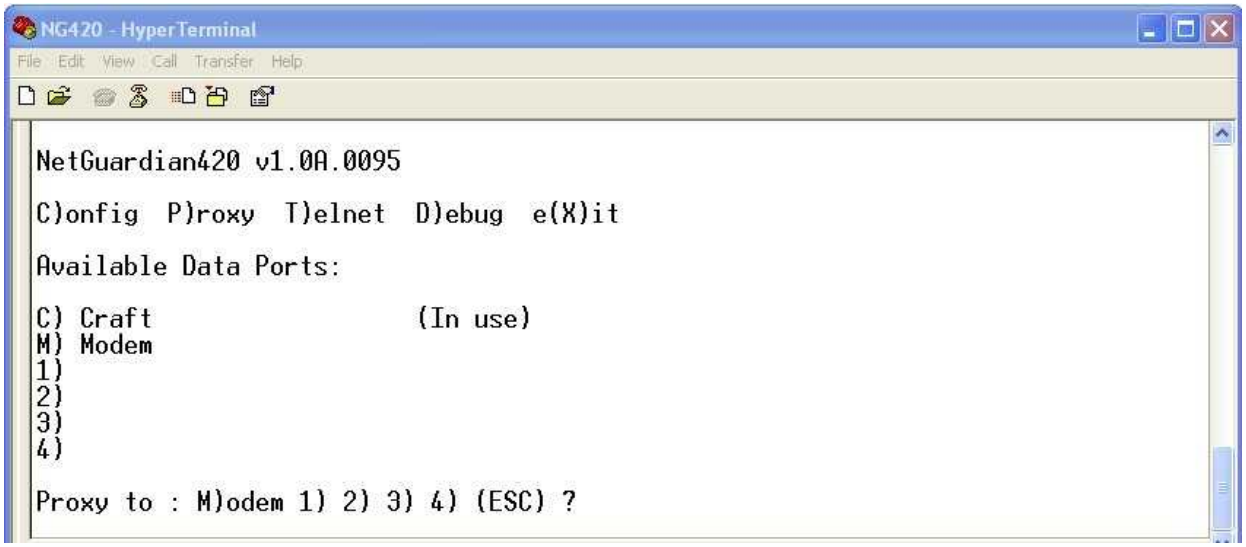

A)larms R)elays a(N)alogs E)vent log a(C)cum. Timer
B)AC P)ing targets p(O)rts S)ystem (ESC) ? S
ID Description Status
17 Timed Tick Clear
18 Exp.Module Callout Clear
19 Network Time Server Clear
20 Accumulation Event Clear
33 Unit Reset Clear
36 Lost Provisioning Clear
37 DCP Poller Inactive Clear
38 LAN not Active Clear
41 Modem not Responding Clear
42 No Dialtone Clear
43 SNMP Trap not Sent Clear
44 Pager Que Overflow Clear
45 Notification Failed Clear
46 Craft RcvQ Full Clear
47 Modem RcvQ Full Clear
48 Data 1 RcvQ Full Clear
ESC to exit Any key to continue_

System Alarms can be viewed from the M)onitor menu > S)ystem option

12.2.1.6 Monitoring Data Port Activity

View the status of the NetGuardian's 4 data ports from the M)onitor menu > p(O)rts option. Enter the number of the port you wish to view and press Enter.

The NetGuardian provides an ASCII description under *Transmit* and *Receive*. Choose a) Transmit to view data transmitted to another device. Choose b) Receive to view data received from another device. See Appendix, "ASCII Conversion," for specific ASCII symbol conversion.



Data port activity can be viewed from the M)onitor menu > p(O)rts option

12.2.1.7 Monitoring the Accumulation Timer

The Accumulation Timer keeps a running total of the amount of time a point is in an alarm state. An alarm point that exceeds a user defined threshold will trigger a Accumulation Event system alarm. Refer to Figure 13.3.1.7.1. and Table 13.3.1.7.A to define the accumulation timer.

```
C)onfig  P)roxy  T)elnet  D)ebug  e(X)it

E)dit  M)onitor  P)ing  S)tats  T)une Modem  R)eset Port (ESC) ? M

A)larms  R)elays  a(N)alogs  E)vent log  a(C)cum. Timer
  B)AC  P)ing targets  p(O)rts  S)ystem (ESC) ? C

Accumulation Timer: enabled
 Display Reference: 1
   Point Reference: 11
 Point Description:
      Point Status: Clear
   Event Threshold: 00:01:01 (dd:hh:mm)
  Accumulated Time: 00:00:00 (dd:hh:mm)
 Accumulated Since: 22-July-2001 03:16

R)eset AccTmr (ESC) ?
```

Monitor and reset the Accumulator Timer

Field	Description
Display and Point	Indicates which alarm point is to be monitored.

Reference	
Point Description	The user-defined description of the monitored alarm point.
Point Status	The current status of the monitored point.
Event Threshold	Amount of time allowed to accumulate before the system alarm, "Accumulation Event" is triggered. **Note:** Maximum is 45 days.
Accumulated Time	The total time the monitored point has been in an ALARM state.
Accumulated Since	Indicates the last time the accumulation timer was reset.
Reset Accumulation Timer	Selecting this option will reset the timer.

Field descriptions in the Accumulator Timer Settings

12.2.2 Viewing Live Target Pings

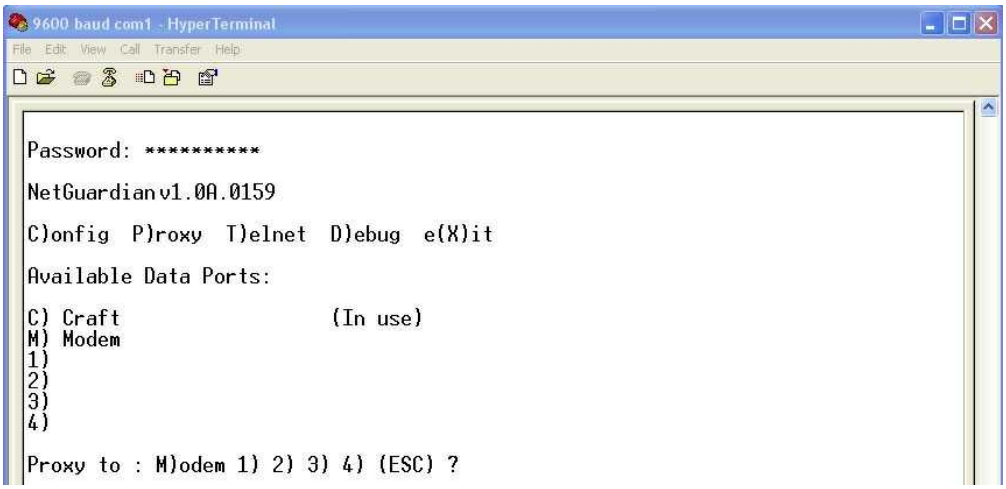
Choose P)ing to ping any of the NetGuardian's user defined IP addresses. Then enter the ID number (1-32) of the IP address or enter any IP address to ping.

Continuously ping an IP address that has been defined in the NetGuardian's ping table

12.2.3 Proxy Menu

You can create proxy connections to reach-through to the craft port, modem port or any of the other eight serial ports from the P)roxy menu. You'll be able to monitor and control additional devices via proxy connection to the NetGuardian. Data presented and handshaking will be specified by the connected device.

To cancel the proxy connection wait a half second, then quickly type @@@ and press ENTER.

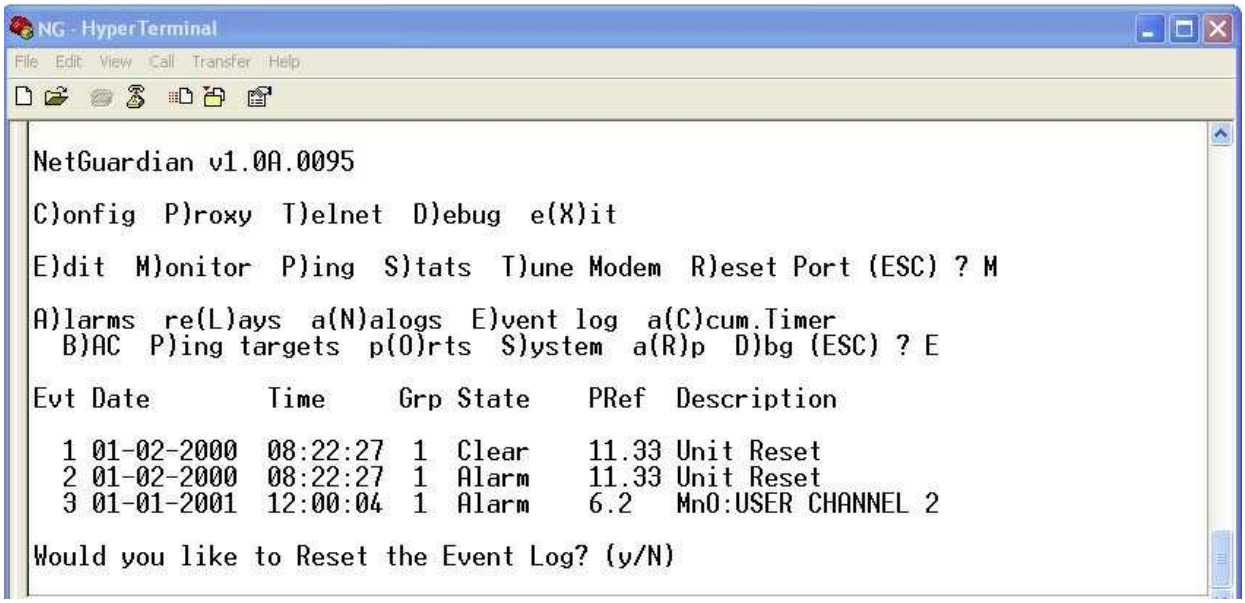


Access devices connected to the eight data ports on the back panel through M)onitor menu > P)roxy option

12.2.4 Event Logging

Choose E)vent log to view the up to 100 events posted to the NetGuardian; including power up, base and system alarms, ping alarms, analog alarms, and controls. Posted events for the various alarms include both alarm and clear status. Refer to Table 13.3.4.A for event log field descriptions.

Note: All information in the event log will be erased upon reboot or a power failure.


NG - HyperTerminal
File Edit View Call Transfer Help
NetGuardian v1.0A.0095
C)onfig P)roxy T)elnet D)ebug e(X)it
E)dit M)onitor P)ing S)tats T)une Modem R)eset Port (ESC) ? M
A)larms re(L)ays a(N)alogs E)vent log a(C)cum.Timer
B)AC P)ing targets p(O)rts S)ystem a(R)p D)bg (ESC) ? E
Evt Date Time Grp State PRef Description
1 01-02-2000 08:22:27 1 Clear 11.33 Unit Reset
2 01-02-2000 08:22:27 1 Alarm 11.33 Unit Reset
3 01-01-2001 12:00:04 1 Alarm 6.2 Mn0:USER CHANNEL 2
Would you like to Reset the Event Log? (y/N)

Monitor the last 100 events recorded by the NetGuardian from the M)onitor menu > E)vent log option

Event Log Field	Description
Evt	Event number (1–100)
Date	Date the event occurred
Time	Time the event occurred
Grp	Alarm Group
State	State of the event (A=alarm, C=clear)
PRef	Point reference (See Appendix A for display descriptions).
Description	User defined description of the event as entered in the alarm point and relay description fields.

Event Log field descriptions

12.2.5 Backing Up NetGuardian Configuration Data via FTP

1. From the Start menu on your PC, select RUN.
2. Type "ftp" followed by the IP address of the NetGuardian you are backing up (e.g. ftp 126.10.120.199).
3. After the connection is made press Enter.
4. Enter the password of the NetGuardian (default password is dpstelecom), then press Enter.
5. Type "binary" and press Enter (necessary for NetGuardian file transfer).
6. Type "lcd" and press Enter (this allows you to change the directory of your local machine).
7. Type "get" followed by the name you wish to define for the NetGuardian backup file. Add the extension ". bin" to the file name (e.g. get ngdbkup.bin) and press Enter.
8. After reloading, type "bye" and press Enter to exit.

Note: The backup file name can have a maximum of eight characters before the file extension.

12.2.5.1 Reloading NetGuardian Configuration Data

1. From the Start menu on your PC, select RUN.
2. Type "ftp" followed by the IP address of the NetGuardian you are backing up (e.g. ftp 126.10.120.199).
3. After the connection is made press Enter.
4. Enter the password of the NetGuardian (default password is dpstelecom), then press ENTER.
5. Type "binary" and press Enter (necessary for NetGuardian file transfer).
6. Type "lcd" and press Enter (this allows you to change the directory of your local machine).
7. Type "put" followed by the name you defined for the NetGuardian backup file and press Enter (e.g. put ngdbkup.bin).
8. Type "literal REBT" to reboot the NetGuardian.
9. After reloading, type "bye" and press Enter to exit.

12.2.6 Debug Input and Filter Options

Debug Input Options	
ESC	Exit Debug
B	Show BAC status points
T	Show task status
U	Show DUART information
R	Show network routing table
X	Clear debug enable bitmap. Turn all debug filters OFF
?	Display Options
Debug Filter Options:	
a	(1) Alarm toggle switch. Shows posting of alarm data
A	(2) Analog toggle switch. Shows TTY interface debug
c	(3) Config toggle switch. Shows TTY interface debug
C	(4) Control relay toggle switch. Shows relay operation
d	(5) DCP responder toggle switch. Shows DCP protocol
D	(6) Device toggle switch. Shows telnet and proxy information
e	(7) Expansion poller toggle switch. Shows NGDdx polling
E	(8) ECU Interrogator toggle switch. Shows BAC processing
f	(9) FTP Command toggle switch. Shows command string parsing
F	(10) FTP Data toggle switch. Shows FTP Read / Write
G	(11) GLD poller toggle switch. Shows GLD polling
h	(12) HTML debug switch. Shows Web Browser processing
H	(13) HWACS debug switch. Shows hardware access operation
i	(14) PING toggle switch
k	(15) Socket toggle switch. Shows current dcu resources
l	(16) LED toggle switch. Shows current LED state
L	(17) LCD display toggle switch. Shows LCD control and text
m	(18) Modem toggle switch. Shows modem vectored initialization
M	(19) Undefined
o	(20) Osstart toggle switch. Miscellaneous application debug, including NVRAM read and write operation, and event posting
O	(21) Undefined
p	(22) SPORT toggle switch. Port init debug and channeled port debug
P	(23) PPP toggle switch. Shows PPP functioning
q	(24) QAccess toggle switch. Reserved for future use
Q	(25) Undefined
r	(26) Report toggle switch. Shows reporting event activity, including SNMP, pagers, email, etc. Also shows PPP negotiation for NG client PPP mode.
s	(27) SNMP toggle switch. Reserved for future use
S	(28) STAK toggle switch. Shows network processing and IPA of arp requests. Also shows packets discarded by Filter IPA.
t	(29) TERM toggle switch. Shows UDP/TCP port handling. The camera and network time (NTP) jobs also use the TERM toggle switch
V	(30) Undefined
w	(31) HTTP toggle switch. Shows handling of web browser packets
W	(32) WEB toggle switch 2. Dump HTML text from web browser

Table. 13.3.A. *Debug Input and Filter Options*

13 Web Interface

Thet NetGuardian's Web Interface provides access to configure and monitor your NetGuardian.

13.1 Logging on to the NetGuardian

Your NetGuardian must first be assigned an IP address via the TTY interface before you will be able to connect via LAN/WAN using the Web Browser. If you have not yet done this, see **Ethernet Port Setup** in section 12 (TTY Interface) of this manual.

To connect to your NetGuardian:
1. Type the IP address of the NetGuardian in your web browser's address bar
2. Type your password in the password field that appears.

Note: The factory default password is **dpstelecom**.

Upon successfully logging in, you will be brought to the alarm summary screen in monitor mode.

The NetGuardian must be assigned an IP address before you will be able to connect via LAN/WAN using a Telnet client or a Web browser. To connect via LAN, the minimum configuration requires setup of the IP address and subnet mask. Minimum WAN configuration requires that the default gateway be set as well. Follow the instructions below to configure the NetGuardian's IP address, subnet mask, default gateway, trap address, SNMP port number, proxy base, and DHCP option.

13.2 Navigating the Web Interface

The links in the left pane of the web interface allow you to navigate to the monitoring or editing screen you wish to view.

Only links for the mode of operation you are in will be visible in the navigation pane.

The web interface has two modes of operation:
1. **Monitor Mode**, in which you may monitor your unit's alarms and issue controls.
2. **Edit Mode**, in which you may configure the unit

The unit defaults to Monitor Mode upon logging in. Clicking the green **Edit** button in the left pane of the web interface will take you to Edit Mode. From Edit mode, you may revert to Monitor Mode by clicking the blue **Monitor** button.

13.3 Edit Mode

Edit Mode provides the user access to all of the unit's configuration options.

If the **Edit** menu does not appear in the left frame after logging on, another station has already logged on as the primary user or you do not have access to edit the NetGuardian 420 database.

13.3.1 System Settings

From the System screen, you can enter basic user information for person responsible for the NetGuardian and configure basic settings for the unit.

System	
Name	NetGuardian420
Location	
Contact	
Phone	
Features	3955-7B-B995
Serial Number	0 (NOT SET)
Unit ID	0 **(Disabled)**
DCP Port	2001 UDP
DCP Protocol	DCPx
SCAN Unit ID	0 **(Disabled)**
SCAN Serial Port	0
Advanced	
Silence non-reportable system alarms	☐
LCD Point Mode (uncheck for scroll)	☐
DNP Address	202
DNP TCP Port 1	4004
DNP TCP Port 2	22001

Submit Data

Field	Description
Name	Used to set the Name of the Name@Location email address of the person responsible for the NetGuardian. **Note:** Name is the portion of the email address before the @ character.
Location	Used to set the Location Name@Location email address of the person responsible for the NetGuardian. **Note:** Location is the portion after the @ character and should be a host name or an IP address.
Contact	Provide information for how to contact the person responsible for this NetGuardian.
Phone	Enter the contact's telephone number.
Features	Used for entering feature codes for future upgrade features. Do not enter anything in this field unless so instructed by DPS Telecom
Unit ID	Enter a user definable ID number for this NetGuardian (DCP Address).
DCP Port	Enter the DCP Port for this NetGuardian. (1-8 serial otherwise UDP/IP Port) **Note**: DCPe added to the list of DCP protocols.
DCP Protocol	Choose between DCPx, DCPf, or DCPe.
Silence non-reportable system alarms	Check the box to silence alarms not applicable to your configuration. Example: This NetGuardian is not setup to send SNMP traps. Check this box to avoid receiving a failure notification for system alarm 13 (SNMP Trap not sent).
LCD Point Mode	Check this box to have the front panel LCD operate in "Point Mode". In this mode, only the points in alarm are displayed on the screen, instead of the full alarm descriptions. Point numbers for discrete alarms, analog threshold crossings, and latched relays will appear on the LCD.
DNP Address	The DNP3 unit address that the NetGuardian 420 will respond to. An address of 0 disables DNP3 responding.
DNP TCP Port 1	The TCP port that the NetGuardian 420 will listen on for DNP3 polling.
DNP TCP Port 2	The secondary TCP port that the NetGuardian 420 will listen on for DNP3 polling.

System fields

Once you've entered your information, click **Submit Data** to commit the data to the NetGuardian.

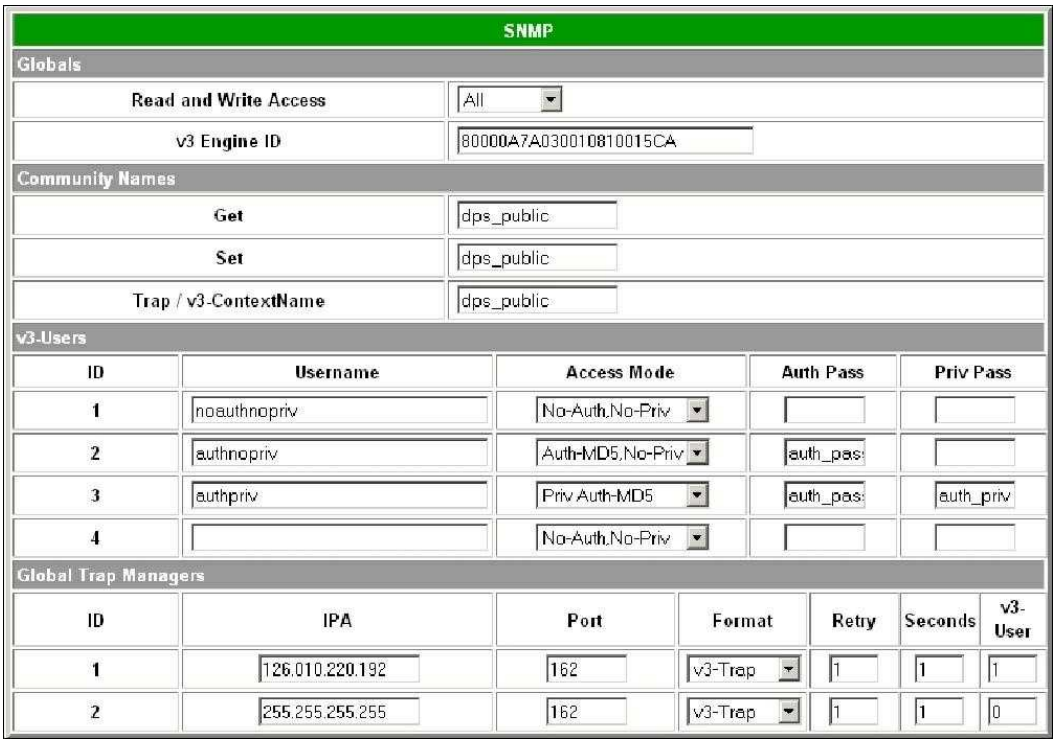
13.3.2 Defining SNMP Parameters

Access the **Edit > SNMP** link to view and edit your unit's SNMP settings.

To define your NetGuardian SNMP parameters:

1. From the **Edit** menu choose SNMP.
2. If you wish to restrict **Read and Write Access** to **All**, **v1-Only**, **v2c-Only,** or **v3-Only**, choose the appropriate option from the drop down dialog box..
3. Enter the community name for SNMP GET requests.
4. Enter the community name for SNMP SET requests.
5. Enter the community name for SNMP TRAPs.
6. If using SNMPv3, enter usernames and access information in the v3-User's section.
7. Define the **IP** address of your trap managers. Set to 255.255.255.255 if not using.
8. Define the **UDP** port set by the SNMP managers to receive traps; usually 162.
9. Select the Format in which you want your traps to be sent to your managers.
10. Click **Submit** to save your system information settings.

For more information on the above steps, see the field descriptions for the Edit SNMP screen in the table below.



SNMP Menu

Globals	
Read and Write Access	This field defines how the NetGuardian unit may be accessed via SNMP. This can be set to the following: • All- Allows you to read or write using any version of SNMP (v1, v2c, v3) • Disabled- Restricts all access to unit via SNMP • v1-Only- Allows SNMPv1 access only • v2c-Only- Allows SNMPv2c access only • v3-Only- Allows SNMPv3 access only
v3 Engine ID	Specifies the v3 Engine ID for your NetGuardian device. DPS recommends using the default ID for the unit, which is automatically generated by the unit. The default ID is generated according to RFC3411 and is based on the unit's unique MAC address and DPS Telecom's SNMP enterprise number. **Note:** To have the unit generate a unique Engine ID, clear the **v3 Engine ID** field and press the **Submit** key.
SNMP Communities	
Get	Community name for SNMP requests.
Set	Community name for SNMP SET requests.
Trap / v3 Context Name	Community name for SNMP TRAP requests. In SNMP v3, defines the context name field of a v3-Trap. **Note:** Make sure that your community strings match those used by the SNMP manager. In v1 and v2c, community strings are security passwords; if the strings do not match, the SNMP manager will not accept Traps from the NetGuardian. Community strings are case sensitive.
v3-Users	
ID	The user number designated for a v3-user. The NetGuardian supports up to four

	v3-User profiles.
Username	The name of the user for which an SNMPv3 management operation is performed.
Access Mode	This identifies the security modes available when SNMPv3 is utilized. The modes are as follows: • **No-Auth, No-Priv-** This access mode does not require authentication and does not require encryption. This mode is the least secure and is comparable to v1 and v2c. • **Auth-MD5,No-Priv-** Provides authentication based on the MD5 algorithm and does not require encryption. • **Auth-SHA,No-Priv-** Provides authentication based on the SHA algorithm and does not require encryption. • **Priv Auth-MD5-** Provides authentication based on the MD5 algorithm and provides DES 56-bit encryption based on the CBC-DES standard. • **Priv Auth-SHA-** Provides authentication based on the SHA algorithm and provides DES 56-bit encryption based on the CBC-DES standard.
Auth Pass	This field contains the password used with either MD5 or SHA authentication algorithms.
Priv Pass	This field contains the password used with privatization encryption.
Global Trap Managers	
IPA	Defines the SNMP trap manager's IP address. Set to 255.255.255.255 if not using.
Port	The SNMP port is the UDP port set by the SNMP manager to receive traps, usually set to 162.
Format	Select between v1-Trap, v2c-Trap, v2c-Inform, or v3-Trap.
Retry	Number of times the NetGuardian will resend SNMP v2c-Informs
Seconds	Time interval in seconds between attempts to resend SNMP v2c-Informs.
v3-Users	Association to the v3-User Table is made to specify the username, security mode, and passwords that should be used for sending a v3-Trap.

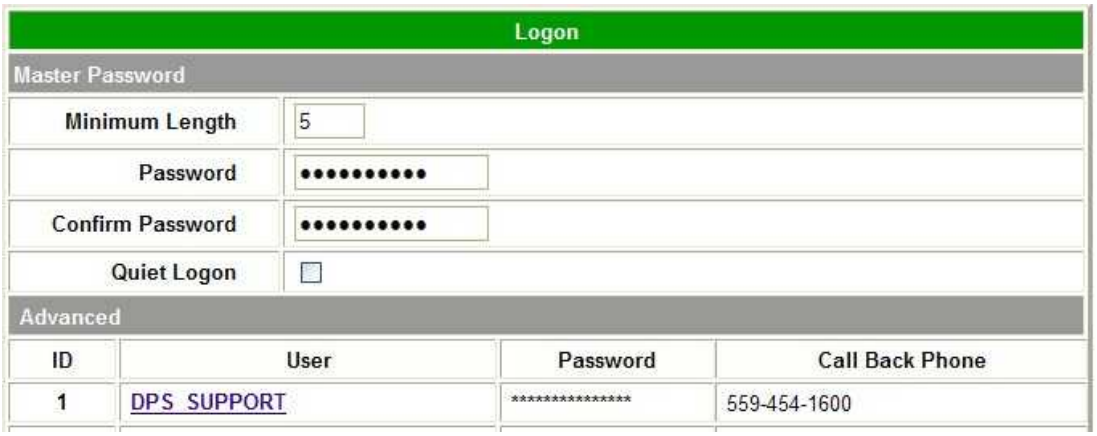
Fields in the Edit > SNMP settings

If you are using SNMPv3, any changes to the Engine ID or passwords will require a reboot. At bootup,you may experience a slight delay while the authorization and privatization keys update.

13.3.3 Controlling Access to the NetGuardian

13.3.3.1 Logon Settings

From the Logon screen, you can change basic logon information for the NetGuardian and create up to 16 unique user profiles each with individual rights to access the NetGuardian.



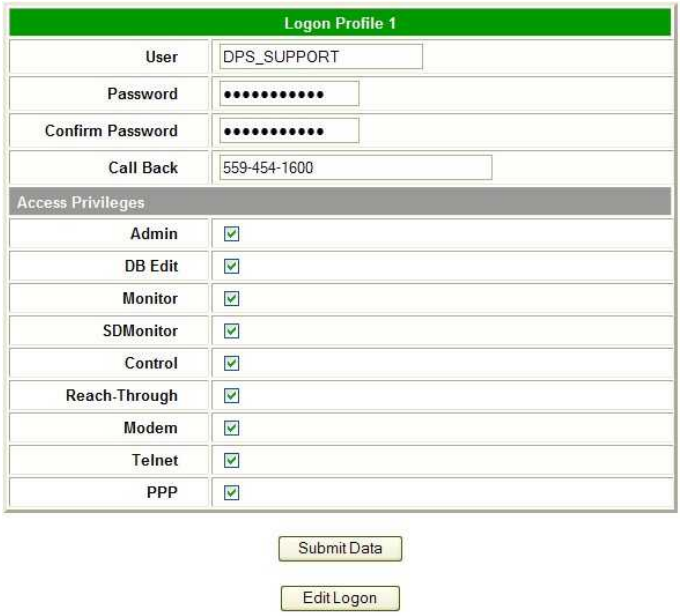
To change the Master password for the unit:
1. Set the minimum password length in the **Minimum Length** field.
2. Enter your new password and confirm the password in the appropriate fields.
3. Check the box if you wish to enable **Quiet Logon.** Quiet Logon keeps the user ID and Password fields from appearing when a user attempts to login to the TTY interface adding another layer of security should anybody mistakenly or maliciously attempt to access your NetGuardian.

To create or edit user profiles, click on the link in the **User** field. By default, the link will read **Available**.

13.3.3.2 Logon Profiles and Access Rights

The NetGuardian 420 allows you to setup up to 16 distinct user profiles and restrict and enable access rights to the NetGuardian based on those profiles.

Note: If you reach the Logon Profile screen by accident, you may return to the previous screen by clicking the back button on your browser, Logon from the navigation links in the left pane of the web interface, or by clicking **Edit Logon** at the bottom of the Logon Profile screen.



Logon Profile Configuration Screen

From the User Profile (1-16) screen, you can configure individual user profiles.

1. Enter a User ID in the **User** field
2. Enter and confirm the User's password in the appropriate fields
3. In the **Call Back** feature, enter the phone number the NetGuardian will use to call-back the user's modem.
4. Set **Access Privileges** for the user.

Profile Field	Access Privilege Descriptions
Admin	Enables the user to add/modify logon profiles and NetGuardian password information.
DB Edit	Enables the user to perform database edits in the NetGuardian.
Monitor	Enables the user to have Monitor access of the NetGuardian.
SDMonitor	Enables the user to view serial port buffers.
Control	Gives the user the ability to issue controls. This also automatically activates Monitor.
Reach-Through	Enables the user to achieve reach-through (Proxy) access.
Modem	Enables the user to call into the unit.
Telnet	Enables the user to have Telnet access to the unit.
PPP	Enables the user to access the PPP server with the user defined password.

Access Privilege descriptions

When you've finished creating or editing a user profile, click **Submit Data.**

13.3.3.3 Filter IPA Config and Operation

The Filter IPA table allows you to increase the NetGuardian's network security by allowing or blocking packets from specified IP addresses. Addresses which appear in the table will be processed by the NetGuardian. Defined IP addresses associated with network cameras or the network time server are automatically processed and will not be filtered out by this feature. Broadcast packets of 255.255.255.255 and ARP requests for the NetGuardian IP address are also not filtered.

1. From the **Edit** menu select **Filter IPA**.
2. A warning prompt will appear. Click **OK** to continue.

Microsoft Internet Explorer
Changing IPA Filter settings may make this unit unreachable from the LAN!
Please take caution and only Enable the IPA Table after submitting and verifying your other Filter IPA settings.
OK

Filter IPA warning prompt

Select Filter IPA from the Edit menu to configure your Filter IPA table

3. Click the checkbox to **Enable IPA Table.**
4. Click the **Block These Addresses** if you wish to block only the addresses listed in the table. If you wish to allow only those IP Addresses listed in the table, do not check this box.
5. Enter the IP address of the machine(s) you would like to give access to the NetGuardian.
6. Click **Submit** to save the configuration settings.

Hot Tip!

Entering a zero in any of the octet fields will declare that part of the octet to be a wildcard.

WARNING: Does not work with networks that assign IP addresses. Use the wildcard field to open an entire subnet.

13.3.3.4 Radius Authentication Settings

RADIUS (Remote Authentication Dial In User Service) is an industry-standard way to manage logins to many different types of equipment in one central location. The NetGuardian 420 connects to your central RADIUS server. Every time a device receives a login attempt (usually a username and password), it requests an authentication from the RADIUS server. If the username & password combination is found in the server's database, an "access granted" reply is sent back to the unit, allowing the user to connect.

RADIUS configuration screen

*RADIUS server prompt for Username **and** Password.*

To configure RADIUS authentication for your NetGuardian, input the appropriate information in the following fields:

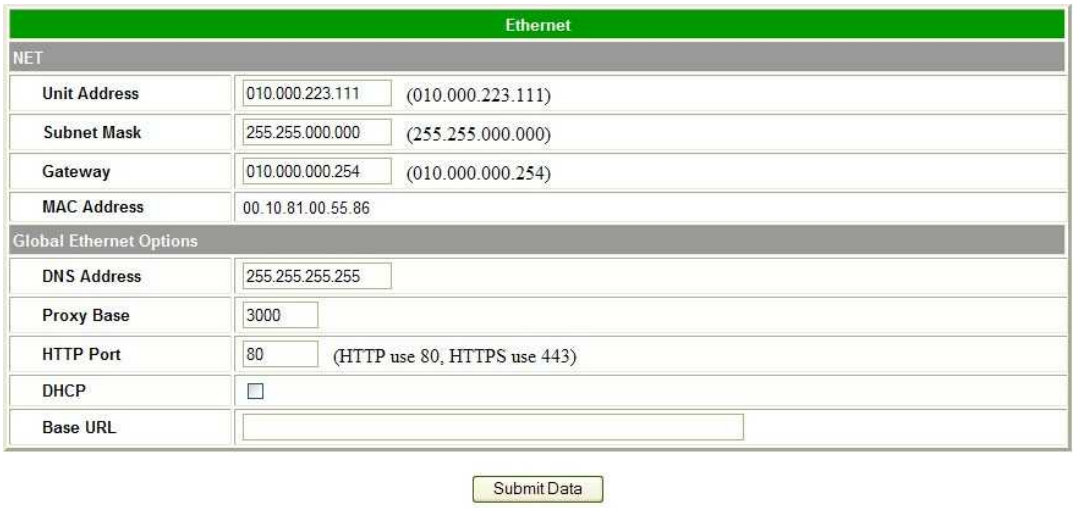
Global Settings	
Retry	Enter the number of times the RADIUS server should retry a logon attempt
Time-out	Enter in the number of seconds before a logon request is timed out
Servers 1 / 2	
IPA	Enter the IP address of the RADIUS server
Port	Port 1812 is an industry-standard port for using RADIUS
Secret	Enter the RADIUS secret in this field

After successfully entering the settings for the RADIUS server, the NetGuardian Web Browser will prompt users for both a Username and Password, which will be verified using the information and access rights stored in the RADIUS database.

RADIUS logons **are** case-sensitive. If the RADIUS server is unavailable or access is denied, the master password will work for craft port access only. Also, the "dictionary.dps" files (included on the Resource Disk) needs to be loaded on the RADIUS server for access-right definition. If RADIUS is enabled on the NetGuardian, local authentication will not be valid.

13.3.4 Ethernet Settings

From the **Ethernet** screen, you can configure information for your NetGuardian 420's ethernet ports.



To change Ethernet information, enter information in the appropriate fields and click **Submit Data**:

Field	Description
Unit Address	IP address of the NetGuardian
Subnet Mask	A road sign to the NetGuardian telling it whether your packets should stay on your local network or be forwarded somewhere else on a wide area network.
Default Gateway	An important parameter if you are on a network that is connected to a wide area network. It tell the NetGuardian which machine is the gateway out of your local network. Set to 255.255.255.255 if not using a gateway.
MAC Address	Hardware address of the NetGuardian (not editable, for reference only).
DNS Address	IP address of the domain name server. Set to 255.255.255.255 if not using.
Proxy Base	Defines the NetGuardian TCP ports used by data ports 1-8 (serial ports). Data port 1 receives the port number entered here. Data ports 2-8 receive the next 7 port numbers in ascending order. (i.e. TCP port 3000 through port 3007 at the IP address of the NetGuardian).
HTTP Port	Enter 80 if using HTTP, 443 if using HTTPS
DCHP	Toggles the Dynamic Host Connection Protocol On or Off
Base URL	The Base URL is the destination website address or the alarm point description hyperlinks. See Section "Using the Base URL Field."

Field Descriptions on the Ethernet Screen

13.3.4.1 Using the Base URL Field

The NetGuardian allows users to turn each alarm point description into a hyperlink. When utilized, the alarm description for each alarm point that appears in the monitor mode (for base alarms, ping targets, or system alarms) becomes a link that directs technicians/managers to specific Web pages or to other files viewable by a Web browser. This allows users to create easily accessible informational databases on how to handle specific alarm conditions or other instructions. The hyperlinked page or file will be displayed in the main window frame of the NetGuardian Web browser. Follow the directions below to create hyperlinks for alarm point descriptions.

1. From the **Edit** Menu select **Ports**. Scroll down to the **Base URL** field, see Figure 2.5.

2. Enter your base URL (e.g. **http://www.dpstelecom.com**). The NetGuardian creates the links from the alarm point descriptions based on the URL. Once the base URL is entered, the NetGuardian automatically attaches a unique suffix to each alarm point. For example, if the base URL is **http://www.dpstelecom.com** the link for the base alarm at point 1 would be **http://www.dpstele.com/base1.html**, Base Alarm Point 2 would be **http://www.dpstele.com/base2.html**, and so on.

3. To add a suffix other than `html` to the hyperlinks, insert the text **&pntID;** into the base URL. This allows the user to specify the extension. For example, if the base URL is **http://www.dpstele.com/&pntID;.pdf**, the link for the base alarm at point 1 would be **http://www.dpstele.com/base1.pdf/.**

Hot Tip!

Any file type that is viewable in your Web browser (e.g. word document, PDF, txt, etc.) is a linkable file.

4. The same link structure applies to the Ping Alarms, System Alarms, and Analog Alarms fields. See Table 2.D for specific URL extension link information.

Alarm Page	Base URL web page link*
Base Alarms	Base1.html - Base20.html
Ping Alarms	Ping1.html - Ping32.html
System Alarms	System1.html - System64.html
Analog Alarms	Analog1.html - Analog8.html

Table 2.D. *Specific link extensions*

* Using the **&pntID;** code in the base URL enables you to link to any file type viewable in your Web browser.

13.3.5 Configuring Ports

You'll configure your unit's modem and terminal server ports from the **Edit** menu > **Ports** screen.

13.3.5.1 Modem Settings

To configure your NetGuardian for PPP or Dial-up access, you may need to enter information in the Modem fields on the **Ports** screen.

To configure the modem port settings.

1. In the **Ring Count** field enter the number of rings before answering. (Default = 1)
2. The **Dial Init** and the **Answer Init** fields can be used if any other modem initialization settings need to be set. For example, the modem can be set to ignore the dial-tone by entering a character code in either the Answer Init (into the NetGuardian) or the Dial Init (out from the NetGuardian).
3. Click **Submit Data** to save your modem port settings.

Change the modem settings from the Edit menu > Ports screen

Command	Description	
A	Answer command	
Bn	Select communications standard	
D	Dial	
	P	Pulse dial
	T	Tone dial
	R	Connect as answering modem
	W	Wait for dial tone
	,	Pause for the duration of S8
	@	Wait for silence
	!	Switch hook flash
	;	Return to the command state
En	Command echo	
Hn	Switch hook control	
In	Modem identification	
Ln	Speaker volume	
Mn	Speaker activity	
On	Online	
Qn	Responses	
Sr?	Interrogate register	
Sr=n	Set register value	
Vn	Result codes	
Xn	Result code set	
Z	Reset	

Modem commands may vary. See your modem user manual for commands specific to your modem.

If you set the ring count to 0, the NetGuardian will still be able to dial out for notifications, but will NEVER answer an incoming call.

13.3.5.2 Data Port Settings

Data port settings can be configured in the **Edit** menu > **Ports** screen.

To configure your data ports:

1. From the **Ports** window, scroll down to the **Data Ports** section.
2. Enter a description for each port with a connected device. You can configure baud rate, word format, and to ignore or remove CR/LF (carriage return/line feed) characters in either the input or output data stream for each port.
3. Click on the link in the **Type** field to choose the data port type. Advanced settings - baud rate, WFmt, CR/LF Mode, and RTS Times - can also be configured when you select an appropriate data port type. (See the following section for details.)
4. Under the options heading, enter in the appropriate number of GLDs (1-12) or NetGuardian Discrete Expansions (1-3) installed. Entering zero disables these options. If connecting more than 3 GLDs, the baud rate must be set to 9600.

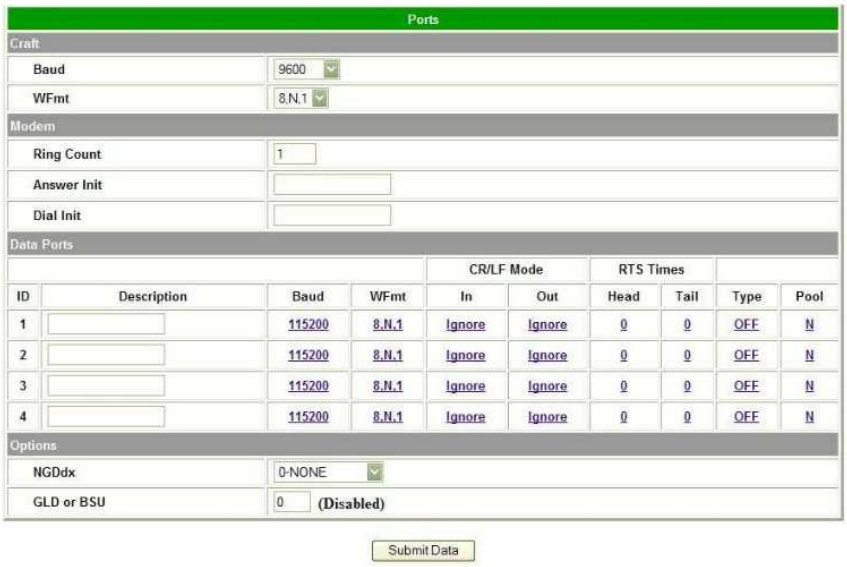
Note: Your NetGuardian's expandability may depend on your unit's availability of RS-232 and RS-485 ports. Normally, NetGuardian expansion units are installed on port 3.

Hot Tip!

NGDdx is an abbreviation for "NetGuardian Expansion." Expansion units enable you to scale from 20 base alarms and 4 base relays to a maximum of 164 alarms and 28 relays. In addition to standard

DX units, you can use the NG480 (configured as a DX) as an expansion unit. The NG480 will give you an additional 80 alarms and 4 relays. You also have the option of adding the NetGuardian E16 DX, giving you 16 more alarm points and 16 more controls.

Note: You can have either 1 NG480 or 1 to 3 NGDdx units. You cannot have both at the same time.



Configure the data port parameters from the Ports screen

13.3.5.2.1Data Port Types

Each of the NetGuardian's 8 data ports can be configured with different functions:

TCP
Makes reach-through available at TCP ports (Telnet).

RTCP
Raw TCP (negates Telnet negotiation). The RTCP (Raw TCP Data Port) negates Telnet negotiation and will allow all characters (including [FF]) to pass straight through from IP to serial or serial to IP.

HTCP
High speed TCP port (only 1 HTCP port is available). An HTCP, or High-speed TCP data port, which operates in Telnet Raw mode, is essentially the same as a RTCP port except that it has better performance and is more robust when transferring streaming data (like a data file). Unlike RTCP ports, the user can only assign one port as HTCP.

PTCP
Permanent TCP (during a proxy connection, the connection will never time out).

SPS8
Serial Port Switch 8. The Serial Port Switch 8 is an external device hub that allows the connection of up to eight serial port devices to a single NetGuardian data port. When an SPS8 port is selected, the NetGuardian will negotiate the connection for the user. To break the SPS8 connection and return to the normal NetGuardian interface, type @@@ and press Enter.

Hot Tip!

SPS8 ports do not support direct proxy. You must navigate via the TTY menu. If interfacing a T/Mon to SPS8 through a NetGuardian, set the port type to **TCP**.

UDP
Makes reach-through available at UDP ports (up to 4 UDP ports available).

CHAN
Creates logical bridge to odd/even partner. The odd/even partners are pairs of 1-2 and 3-4. This allows the NetGuardian to view communication traffic in either direction when inserted in the serial communication path between two devices. This is accomplished by going "in" to the NetGuardian with one device and "out" to the other device from the odd/even partner port. Data is passed directly from one port to its odd/even partner without being altered in any way. This ability greatly simplifies troubleshooting communication problems by isolating the non-communicating device.

When **CHAN** is selected, the NetGuardian automatically activates the odd/even partner as **CHAN**. Baud rates for the odd/even pairs can be set to any available rate except for any combination of 19200 and 38400 between the two ports. Use "SPO" filter debug to analyze protocol traffic in a terminal.

CRFT
Causes the data port to have the same functionality as the front panel craft port.

CAP
Allows the user to capture debug information. The debug information is stored in the receive queue of the NetGuardian (See section "Monitoring Data Port Activity" for more information). This is used primarily as a troubleshooting feature.

ECU
For use if an ECU is connected to this port (see section "Building Access Controller").

13.3.5.2.2Direct and Indirect Proxy Connections

The NetGuardian supports both direct and indirect proxy connections. In a direct proxy connection, the user enters an IP address and port number to Telnet directly to a TCP serial port. In an indirect connection, the user navigates the TTY menu to select a proxy port. Because the TTY interface is password protected, thus providing greater security, indirect connections are preferred. Some users prefer to disable direct proxy for all connections in order to enforce the password security provided by the TTY interface.

To disable proxy connections you may either:
1. Set the proxy port to an uncommon value.
2. Set the data ports to **off** in the **Type** field. When set to **off**, the port is no longer associated with a TCP socket, which effectively disables the port from direct access. This is a more secure and convenient method of disabling proxy access.

13.3.6 Configure Alarm Notifications

The **Edit** menu > **Notification** screen allows you to configure methods for alarm notification. The following sections will explain how to configure individual methods for alarm notification.

Multiple notification methods and group assignments are configured from the Notification screen

Pager Format	Description
Alphanumeric Paging	Format recognizes numbers, letters, and symbols. Can receive information including alarm point addresses, alarm descriptions, time of alarms, and alarm state a.k.a TAP.
Numeric Paging	Format recognizes numbers only. Message is reported in the following order: [IP]*[Display] [Address]*[State]. When read on the pager it appears as follows: 192.168.1.100 99.01.01.01
Text Paging	Can receive information including alarm point addresses, alarm descriptions, time of alarms, and alarm state. May be accessed using a terminal.
T/Mon Paging	The T/Mon may receive alarm information from the NetGuardian via dial-up and display alarm information, alarm description, and threshold status. (Only activates if DCP Poller is inactive)
TCP (ASCII) Paging	Alarm status notification via multiple TCP or HTCP ports. Connection from a higher level master must be established for alarm notification.
Email/SMTP Paging	Provides alarm notification via email, with a description similar to the Alphanumeric pager.
SNMPv1 Paging	May send alarm status to multiple SNMP managers, including the SNMP that alarms are reporting to. The SNMP trap format is v1.
SNMPv3 Paging	May send alarm status to multiple SNMP managers, including the SNMP that alarms are reporting to. The SNMP trap format is v3.
Num17 Paging	Provides alarm notification in a manner similar to that of the Numeric pager. However, Num17 eliminates the (*) symbol from the page. Message is reported in the following order: [IP] [Display][Address][State]. When read on the pager it appears as follows: 192.168.1.100 99.01.01.01
Echo	Allows an alarm point on the NetGuardian to operate a control on another SNMP-enabled, DPS Telecom RTU.

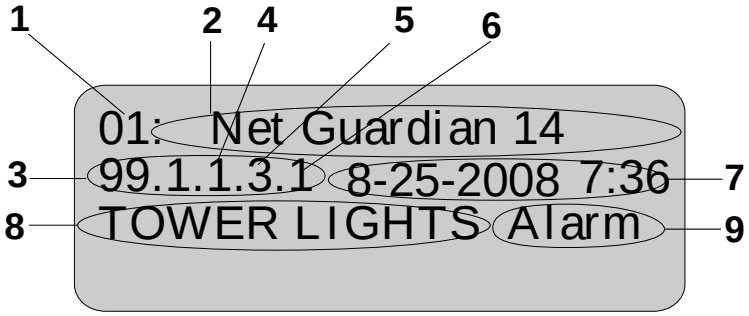
Notification formats

Many cellular carriers offer a TAP gateway to SMS. Check with your carrier to see if you can use a dial-up connection to send SMS messages to your phone. This creates an out-of-band path in the case of a network failure.

13.3.6.1 Alphanumeric Pager Setup

The alpha numeric pager can receive text messages including alarm descriptions, time of occurrence, and point addresses.

Use the following steps to configure the alpha numeric pager settings:
1. Under the **Type** column, select type **Alpha** from the drop-down menu, see Figure 2.14.
2. Enter the phone number of the Alpha numeric pager under the **Phone/Domain** heading.
3. Enter a personal identification number under the **PIN/Rcpt/Port** heading.
4. Set the pager data rate (i.e. 300, 1200, 2400 or 9600). The default baud is 1200.
5. Select a pager word format (Data Bits, Parity, Stop Bits). The default setting is 7,Even,1.



1. Number of pages
2. Unit name
3. Port # and Address
   (Applicable to T/Mon and IAM only)
4. Display number
5. Alarm point number
6. Alarm status: 1=alarm, 0=clear
7. Date and Time NetGuardian sent page
8. Alarm point description
9. Alarm status

Alpha numeric pager description

13.3.6.2 SNPP Notification Setup

Alpha numeric pagers can receive text messages including alarm descriptions, time of occurrence, and point addresses using SNPP.

Use the following steps to configure the alpha numeric pager settings:.
1. Under the **Type** column, select type **SNPP** from the drop-down menu.
2. Use the **Phone** field if a login username and password are required. They must be separated by a colon and be no longer than 29 characters combined. Otherwire, leave this field blank.
3. Enter the numeric pager number under the **PIN/Rcpt/Port** heading.
4. Under the IPA field, enter the static IPA of the SNPP server. Port automatically defaults to 444.

13.3.6.3 Numeric Pager Setup

The numeric pager can receive point addresses of alarms.

Use the following steps to configure the numeric pager settings:
1. Under the **Type** column select **Numeric** from the drop-down menu.
2. Enter the phone number of the numeric pager under the **Phone/Domain** heading, followed by 7 commas (e. g. **555-1212,,,,,,,**). Placing a comma after the phone number initiates a two second pause (per comma). This allows enough time for the pager to answer before the NetGuardian sends the alarm information.

The Baud/Wfmt and IPA fields are not used from numeric pager types.

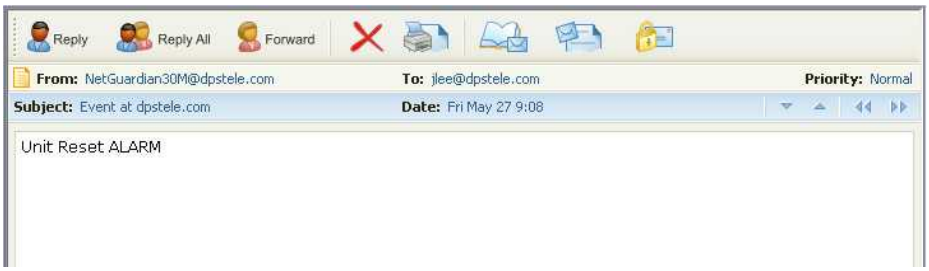
13.3.6.4 Text Paging Setup

Text pages can receive information including the point addresses of alarms, the alarm description, time of the alarm, and state (alarm or clear). The text pages may be viewed using a terminal such as HyperTerminal.

Use the following steps to configure the text paging settings:
1. Under the **Type** column select **Text** from the drop-down menu.
2. Enter the phone number of the text paging device under the **Phone/Domain** heading.
3. Set the pager data rate (i.e. 300, 1200, 2400 or 9600). The default baud is 1,200.
4. Select a pager word format (e.g Data bits: 7 or 8, Parity: none (N), even (E) or odd (O), and Stop Bits: 1). The default setting is 7, Even,1.

To set up text paging from T/Mon see the T/Mon user manual.

13.3.6.5 Email Notification Setup



Email notification from the NetGuardian

The email pager provides alarm notification via email, with a description similar to that of the alpha-numeric pager.

1. Use the following steps to configure the email notification settings:
2. Under the **Type** column, select **Email** from the drop-down menu.
3. Enter the domain name of the email address under the **Phone/Domain** heading. This is the portion of an email address after the @ symbol in **name@domain.com**.

Note: There cannot be any spaces in the domain name.

4. Enter the email recipient's user name under the **PIN/Rcpt/Port** heading. This is the portion of an email address before the @ symbol in the **name@domain.com.**

Note: There cannot be any spaces in the recipient's user name

5. Enter the IP address of the SMTP mail server in the **IPA** field.
6. Click **Submit Data** to save your email notification settings.
7. Click on the **System** link. If you have not done so, set up the "from" address sent in email messages sent from the NetGuardian by entering the appropriate information in the **Name** and **Location** fields. The email notification from the NetGuardian will appear as follows: **name@location**.

Hot Tip!

Most email programs can be set to perform a certain action if a message is received from a specified address, such as moving the message to a special Alarms folder. Use the address entered in the **Systems** screen for such purposes.

8. Click **Submit Data** to save your new system information settings.

The "from" email address is for identification purposes. It is not necessarily a real email address that can be replied to unless one is entered.

13.3.6.5.1SMTP & POP3 Authentication Support

This section contains steps to configure your NetGuardian for SMTP and POP3 Authentication support.

Unauthenticated Emails:
The configuration setup will not change. If you want the email to send to **user@yourdomain.com**, use the following steps:
1. In the **Phone/Domain** field type **yourdomain.com**.
2. In the **Pin/Rcpt** field type **user**.
3. Click **Submit Data** to save the configuration settings.

The "from" location is specified by the system info name and location strings, which also do not change. Use the following steps to configure the "from" location **from@fromdomain.com:**
1. Click on the **Edit** menu > **System** link.
2. In the `Name` field type **from**.
3. In the **Location** field type **fromdomain.com**.
4. Click **Submit Data** to save the new system information settings.

Authenticated Emails:
If you want to send an authenticated email to **user@yourdomain.com** from **from@fromdomain.com**, password **= authentic**, then use the following steps:
1. In the **Pin/Rcpt** field type **authentic**.
2. Click **Submit Data** to save your changes.
3. Click on the **Edit menu > System** link.
4. In the `Name` field type **user**.
5. In the **Location** field type **yourdomain.com.**
6. Click **Submit Data** to save the new system information settings.

13.3.6.6 SNMPv1 Paging Setup

The SNMPv1 paging feature allows you to view alarm status from multiple SNMP managers in addition to the global managers, which are setup from the SNMP menu.

Use the following steps to configure the SNMP paging settings:
1. Under the **Type** column, select **SNMPv1** from the drop-down menu.
2. Set the SNMP port under the **PIN/Rcpt/Port** heading, usually 162.
3. Enter the IP address of the SNMP manager in the **IPA** field.

13.3.6.7 SNMPv3 Paging Setup

The SNMPv3 paging feature allows you to view alarm status from multiple SNMP managers in addition to the global managers, which are setup from the SNMP menu.

Use the following steps to configure the SNMP paging settings:
1. Under the **Type** column, select **SNMPv3** from the drop-down menu.
2. Enter a v3-User ID under the v3-User heading. The values can range from 0-4. These values refer to the **v3-Users** table in the SNMP page. The v3-User association is used to specify username, security mode, and

passwords that should be used for sending a v3-Trap.
3. Set the SNMP port under the **PIN/Rcpt/Port** heading, usually 162.
4. Enter the IP address of the SNMP manager in the **IPA** field.

13.3.6.8 TCP Paging Setup

<MSG_BEG 00001>
VID : DPS Telecom
FID : NetGuardian SNMP v5.0B.3206
SITE: Yale Office
PNT : 99.01.01.01
DESC: RECTIFIER 1
STAT: CLEAR
DATE: 01/01/2001
TIME: 12:17:02
<MSG_END 00001>

Fig. 2.17. *Example TCP message*

Heading	Description
MSG_BEG MSG_END	Sequential message number used to group the message and detect missing messages (e.g. 00001, 00002, etc…).
VID	Vendor ID
FID	NetGuardian Firmware ID.
SITE	NetGuardian system name.
PNT	Point ID (port.address.display.point). See Appendix A for display mapping.
DESC	Description set forth in the Alarm parameters.
STAT	Status of the alarm (Clear or Alarm).
DATE	Date the alarm occurred.
TIME	Time the alarm occurred.

Table 2.H. *TCP alarm message field descriptions*

The NetGuardian offers alarm status notification via multiple TCP ports. When an alarm condition occurs, an alarm condition formatted according to Figure 2.17 will be sent to the specified TCP points for use by a higher level master. This connection must be established by the master. Any applicable alarm activity occurring prior to an established connection will be discarded.

Use the following steps to configure the TCP paging settings:
1. Under the **Type** column, select **TCP** from the drop-down menu.
2. In the **Pin/Rcpt/Port** field enter the NetGuardian TCP port number where alarm messages will be sent (from 1 to 65,536). Multiple ports can be defined by defining multiple pager IDs as TCP pagers and then entering the desired ports.
3. The TCP message can be viewed by a Telnet session by connecting to the NetGuardian's IP address and the TCP port entered in this screen. For example, Telnet to **126.10.220.199 5000** if port 5000 is selected and 126.10.220.199 is the unit's IP address. See Figure 2.17 for an example message and Table 2.H for TCP message format information.

13.3.6.9 NUM17 Pager Setup

The Num17 Pager can receive point addresses of alarms. It is quite similar to the Numeric Paging format in the way it receives and reports alarms. However, on certain pager systems the symbol * will cause a freeze or other undesirable situations. Num17 eliminates the * symbol from the pages it receives and reports alarms as a 17-digit series of numbers.

User the following steps to configure Num17 Pager settings:
1. Under the **Type** column select **Num17** from the drop-down menu.
2. Enter the phone number of the numeric pager under the Phone heading, followed by commas (for example **555-1212,,,,,,,**). Placing a comma after the phone number initiates a two second pause per comma. This allows enough time for the pager to answer before the NetGuardian sends the alarm information. The **Baud/ Wfmt** and **IPA** fields are not used from Num17 pager types.
3. Click **Submit Data** to save the configuration settings.

13.3.6.10 Echo Notification Setup

An Echo notification type enables an alarm point on the NetGuardian to operate a control on another SNMP remote from DPS.

1. From the Notification devices tab, choose **Echo** as the notification Type.
2. Enter the Community Set Name in the Phone/Domain field.
3. Enter the Relay Point Reference in the Pin/Pcpt/Port field. This is entered as:[Port].[Address].[Display].[Relay Point] NOTE: The Port will always be 99, and the address is always 1. Therefore, your entries will always begin with 99.1.
4. The Baud/Wfmt and Group fields will not be used.
5. Under IPA, enter in the IP address of the SNMP-enabled, DPS remote you are setting up to operate its relay.

NOTE: If more than one point is mapped to Echo notification, the OR'ed logic is applied.

13.3.7 Defining Point Groups

Each NetGuardian Alarm point can be assigned to one of eight groups, which are identified with a user-defined label. Once the point groups are defined, the Point Group IDs can be used to group base and system alarms, see section "Configuring Base Discrete Alarms."

Use the following steps to define alarm messages for alarm point groups:

1. To define the point groups, select **Point Group** from the **Edit** menu.
2. Then enter the appropriate descriptions in the **Description**, **When Set** and **When Clear** fields for each point group.
3. Click **Submit Data** to save the point group settings.

Define the Alarm and Clear messages for up to eight different point groups

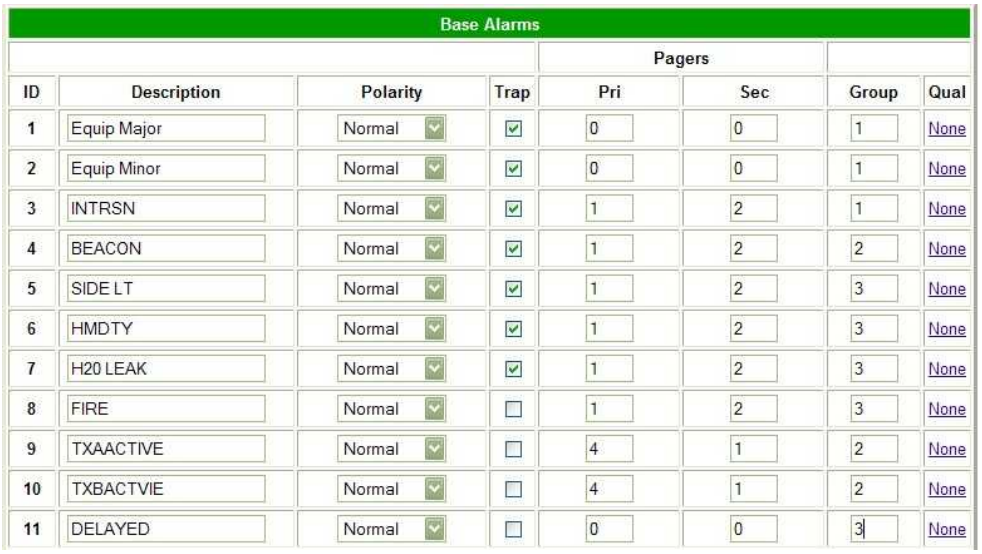
13.3.8 Configuring Base Discrete Alarms

All of the NetGuardian's 20 discrete alarms are configured from the **Edit** menu > **Base Alarms** screen. Descriptions of the alarm point, polarity (normal or reversed), whether to use an SNMP Trap or not, and the primary and secondary pager used to report the alarm, and group assignments, are configured in this screen.

Use the following steps to configure base discrete alarm settings:

1. From the **Edit** menu select the **Base Alarms** link.
2. Enter a description for each discrete input alarm being used in the **Description** field.
3. Under the **Polarity** column, you can choose to reverse the polarity or leave it normal. If you select **Normal**, a contact closure is an alarm. If the Reverse option is selected, the alarm is clear when closed.
4. Select the **Trap** check box to send an SNMP trap for that alarm point in the event of an alarm condition. Leave the box blank if you do not wish the NetGuardian to send an SNMP trap.
5. Set the primary and secondary pagers with a pager ID from your Notification list. (See Section "Configure Notification Methods" for more information.) The NetGuardian will notify both the primary and the secondary notification device when point status changes (both alarm and clear).
6. Under the **Group** column enter the appropriate point group ID. (For more information, see "Defining Point Groups.")
7. Under the **Qual** column click the **None** link to configure an event qualification time setting for the alarm point. The **Event Qual** screen will appear. For more information on the Qual field, see the section titled, "Event Qualification Timers".
8. Click **Submit Data** to save base alarm configuration settings.

The pager device can be an ASCII terminal, T/Mon element manager, email, or multiple SNMP managers as well as an alpha or numeric pager.



Base Alarms

				Pagers			
ID	Description	Polarity	Trap	Pri	Sec	Group	Qual
1	Equip Major	Normal	☑	0	0	1	None
2	Equip Minor	Normal	☑	0	0	1	None
3	INTRSN	Normal	☑	1	2	1	None
4	BEACON	Normal	☑	1	2	2	None
5	SIDE LT	Normal	☑	1	2	3	None
6	HMDTY	Normal	☑	1	2	3	None
7	H20 LEAK	Normal	☑	1	2	3	None
8	FIRE	Normal	☐	1	2	3	None
9	TXAACTIVE	Normal	☐	4	1	2	None
10	TXBACTVIE	Normal	☐	4	1	2	None
11	DELAYED	Normal	☐	0	0	3	None

Configure the 20 discrete alarms from the Base Alarms screen

13.3.9 Configuring System Alarms

System Alarms

			Pagers		
ID	Description	Trap	Pri	Sec	Group
17	Timed Tick	☐	0	0	1
18	Exp.Module Callout	☐	0	0	1
19	Network Time Server	☐	0	0	1
20	Accumulation Event	☐	0	0	1
21	Duplicate IP Address	☐	0	0	1
33	Unit Reset	☐	0	0	1
36	Lost Provisioning	☐	0	0	1
37	DCP Poller Inactive	☐	0	0	1
38	NET 1 is not Active	☐	0	0	1
40	NET Link Down	☐	0	0	1
41	Modem not Responding	☐	0	0	1
42	No Dialtone	☐	0	0	1
43	SNMP Trap not Sent	☐	0	0	1

SNMP Traps and primary or secondary pager devices can be selected for each system alarm

The **System Alarms** screen allows you to individually set the notification method for each system alarm. See the "System Alarms Display Map" in the Reference Section for detailed descriptions of System Alarm Points.

To configure your system alarm notification settings:

1. From the **Edit** menu select the **System Alarms** link.
2. Check the **Trap** box to send an SNMP trap for that alarm point.
3. Set the primary and secondary pagers with a Notification ID from your defined notification list. (See Section "Configure Alarm Notifications" for more information.)

Note: The NetGuardian will notify both the primary and the secondary notification device when point status changes (both alarm and clear).

4. Under the **Group** column enter the appropriate Point Group ID, see section.
5. Click **Submit Data** to save the configuration settings.

13.3.16 Setting Ping Targets

Fig. 2.23. *Configure the ping target parameters from the Ping Info screen*

Each of the 32 ping targets can be provisioned with a description, an IP address, primary and secondary notification devices, and an option to verify connection using SNMPv1 GET.

Note: To set ping response and fail times, see the section titled **Setting System Timers**.

To configure the ping targets:

1. From the **Edit** menu select **Ping Targets.**.
2. In the **Description** field, enter a description of the device to be pinged.
3. In the **IP Address** field enter the IP address of the device to be pinged.
4. Under the **Trap** column check the box to designate that an SNMP trap will be sent when an alarm condition exists. Leaving the box blank indicates that an SNMP trap will not be sent when an alarm condition exists.
5. Set the primary and secondary pagers with a Notification ID from your defined Notification list.

Note: The NetGuardian 420 will notify both the primary and the secondary notification device when point status changes (both alarm and clear).

6. Under the **Group** column enter the appropriate Point Group ID.
7. Under the **SNMP** column check the box to enable pinging of the device using SNMPv1 GETs instead of traditional ICMP. If the box is not checked, the device will be pinged using traditional ICMP.
8. Select the OID to retrieve with the SNMP GET. The following is a list of available MIB variables in the **System OID** field:

   sysDescr, OID .1.3.6.1.2.1.1.1.0
   sysObjectID, OID .1.3.6.1.2.1.1.2.0
   SysUpTime, OID .1.3.6.1.2.1.1.3.0

9. In the **Community** field enter the community string for the SNMP GET request.The community string must match the community string configured in the target device.
10. Click **Submit Data** to save the configuration settings.

13.3.11 Setting the Accumulation Timer

Define the Accumulation Timer settings to send an Accumulation Event alarm

The NetGuardian's **Accumulation Timer** keeps a running total of the amount of time a point is in an alarm state to send an Accumulation Event system alarm once the total time exceeds a defined threshold.

To configure the accumulation timer settings:

1. Go to the **Edit** menu and select the Accum._Timer link.
2. In the **Display Reference** field enter the display number to be monitored.
3. In the **Point Reference** field enter the alarm point to be monitored.
4. In the **Event Threshold** row enter the appropriate running total days, hours and minutes a point is in a alarm state in order to send an accumulation event system alarm.
5. Click **Submit Data** to save the configuration settings.

Accumulated Time indicates the number of days, hours, and minutes the timer's been running. **Accumulated Since** indicates when the Timer started.

Hot Tip!

Only check the **Reset Accumulation Timer** box if you wish to reset the timer.

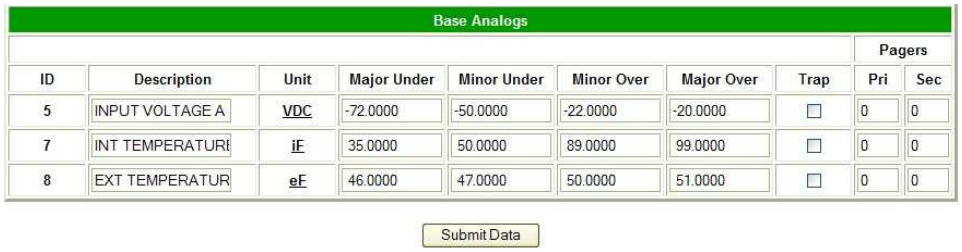
The **Point Description, Point Status, Accumulated Time, and Accumulated Since** fields are not configurable. These fields will show the corresponding data of the point you configure for the accumulation timer after you have hit the **Submit Data** button.

13.3.12 Configuring Analogs

Each of the NetGuardian 420's analog channels must be individually configured to monitor data. The ADCs (analog to digital converters) support a range of –70 to 94 VDC. There are four alarm trip points (thresholds) in ascending order: major under, minor under, minor over, and major over. You can choose the values for each of the thresholds on all channels. As with the other alarms, you can designate whether or not to send an SNMP trap when a threshold is crossed. The primary/secondary pager used to report the alarm is also set here. The thresholds must be set from **Under** to **Over** in either ascending or descending potential (or current) order. Thus the settings of –10, –5, 5 and 10 corresponding respectively to major under, minor under, minor over and major over is valid.

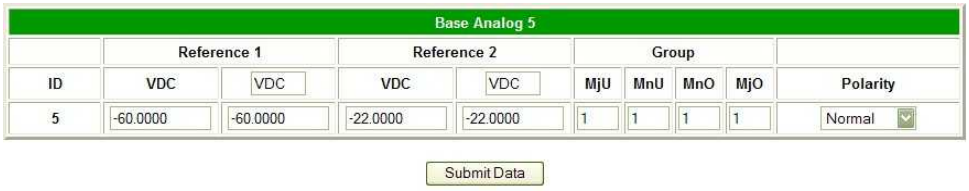
The analog alarms are set to measure voltage by default and the thresholds are reported as "native units." For example, you may set Channel 3 to measure outside temperature. If you were using a sensor with a measurable temperature range between –4° to 167° Fahrenheit (–20° to 75° Celsius). The voltage for that channel varies between 1 and 5 VDC for that sensor, which is to be reported as ° Fahrenheit (native units) where 1 volt represents –4° Fahrenheit and 5 volts represents 167° Fahrenheit.

To change any one analog alarm to measure current instead, a dip switch setting must be changed. Refer to the NetGuardian hardware user manual for details on jumper locations and positions. The jumper inserts a 250 ohm shunt resistor across the input to convert the sensors current output to volts. Use ohms law to find the voltage drop across the 250 ohm shunt resistor (multiply the current by the resistance 250 ohms). Please refer to the operation manual for your sensor to determine any other conversion factors. This will allow you to correctly set the thresholds for **over** and **under** conditions.



The Analog Parameters can be viewed and changed from the Analogs screen

1. From the **Edit** menu click on the **Analogs** link.
2. In the **Description** field enter a description for each analog channel being utilized.
3. Under the **Unit** column, click on the abbreviated units link (e.g VDC, RH, F, etc.).
4. Set **Reference 1** (VDC) to the minimum output (in volts DC) of the analog device being configured.
5. In the box next to **VDC** (the space may already contain the abbreviation VDC) enter an abbreviation for the native units (e.g. RH for relative humidity, F for ° Fahrenheit, etc.).
6. In the box below the abbreviated native unit setting enter the native unit amount that corresponds to the minimum output entered in the previous step.
7. Set **Reference 2** (VDC) to the maximum output (in volts DC) of the analog device being configured.
8. In the box next to **VDC** enter an abbreviation for the native units (e.g. RH for relative humidity, F for ° Fahrenheit, etc.).
9. In the box below the abbreviated native unit setting enter the native unit amount that corresponds to the maximum output entered in the previous step.
10. Enter the Point Group ID designated for each alarm level (MjU = Major Under, MnU = Minor Under, MjO = Major Over, MnO = Minor Under).
11. Click the **Submit Data** button to save the configuration settings.
12. Follow these steps for each analog channel being configured.



Reference 1 and reference 2 correspond to the minimum and maximum output values of your analog device

13.3.12.1 Integrated Temperature and Battery Sensor (Optional)

The optional integrated temperature and battery sensor allows the user to monitor surrounding temperature as well as the unit's current draw. This is only available if the NetGuardian was purchased with this option. If you are using the temperature or battery sensor, you must dedicate an analog port to each one (see user manual for connection information).

CAUTION: Ambient room temperature will be cooler than the NetGuardian integrated temperature.

Temperature Sensor

1. In the **Description** field enter a description in the analog channel you are using for the integrated temperature sensor. 7=internal and 8=external.
2. Under the **Unit** column, click on the abbreviated units link (e.g VDC, RH, F, etc.) to convert the reference units and the native units for that analog channel, see Figure 2.24.
3. In **Reference 1** enter **iF** (integrated Fahrenheit or external Fahrenheit) in the box next to **VDC** (the space may already contain the abbreviation VDC), see Figure 2.24. This enables the NetGuardian's pre-configured temperature settings. Repeat this step for **Reference 2.**
4. Set your desired thresholds.

Battery Sensor

1. In the **Description** field enter a description in the analog channel you are using for the integrated current sensor. 5= Battery A and 6= Battery B.
2. Set your desired thresholds. Be sure to set your thresholds in reference to your NetGuardian's power input (e. g. –24 VDC, –48 VDC, or wide range).

13.3.12.2 Analog Polarity Override

eF : external temperature sensor in fahrenheit or `iC` for celsius
iF : integrated temperature sensor in fahrenheit or `iC` for celsius
oV+ : override polarity VDC to positive
oV- : override polarity VDC to negative

If you have a positive powered NetGuardian, you may want to use this feature if you are using the internal battery sensor. The Web Browser Interface will override **oV+** and **oV-** tags and show `VDC`. So you won't have to view an uncommon looking tag while in monitor mode.

Analog Accuracy:
+/- 1% of analog range.

13.3.12.3 Analog Step Sizes

Analog Step Sizes	
Input Voltage Range	**Resolution (Step Size)**
0-5 V	.0015 V
5-14 V	.0038 V
14-30 V	.0081 V
30-70 V	.0182 V
70-90 V	.0231 V

Analog step sizes

13.3.13 Configuring Control Relays

Configure controls in the Edit menu > Controls screen

The NetGuardian 420's 4 relays can be identified and configured using the **Edit** menu > **Controls** screen.

Relays are normally open (N/O) by default. A circuit board jumper can be changed for each control to make it normally closed (N/C). Refer to

To configure your relays:

1. From the **Edit** menu, select the **Controls** link.
2. In the **Description** field enter a description for each control/relay being used.
3. Set the **Energize State** to either **Normal** or **Inverted**. Selecting **Normal** sets the relay's normal electrical state to **De-energized**. Selecting **Inverted** sets the relay's normal electrical state to **Energized**.
4. Check the **Trap** box to send an SNMP trap for that alarm point. Selecting the box will set that point to send a SNMP trap when the relay is activated, leaving the box blank will set that point to not send an SNMP trap.
5. Under the **Group** column enter the appropriate Point Group ID
6. Click **Submit Data** to save the configuration settings.

Hot Tip!

The Energize State is different than the normal state of the physical contact closure position of each relay, which is determined by circuit board jumpers. This gives you the added benefit of being able to monitor the wire. In the event of a power failure, the relay would de-energize back to it's normal physical contact closure set by the circuit board jumper for that relay. Check your jumper settings and relay connections before setting to Normal or Inverted.

13.3.14 Setting Event Qualification TImers

Event qualification timers allow you to determine a length of time that must pass before an event can occur. For example: you may set a qualification timer that requires an alarm to be set for five seconds before it is reported.

Edit the Even Qualification Timer settings from the Edit > Even Qual screen

To configure Event Qual timers:

1. From the **Edit** menu select from the **Event Qual** drop down menu. The NetGuardian supports up to 128 Event Qualification Timers, which are grouped into sections of sixteen.
2. Enter the display and point number for the point you wish to qualify.

Note: the ID will correspond to Event Qualification. A list of displays and points can be found in Appendix B.

3. In the **Value** field enter the appropriate value (the field handles entries between 1 - 127).
4. Under the **Units** column, click on the drop-down menu and select the appropriate unit of time (sec, min, hour).
5. Under the **Type** column click on the drop-down menu and select the appropriate event type (Alm = alarm, Pri = primary, Sec = secondary).

Note: To delete an entry, set the **Type** to None.

6. When you are done making changes, scroll to the bottom of the page and click **Submit Data**.

CAUTION: Set conditions for alarms are qualified, clear conditions are not.

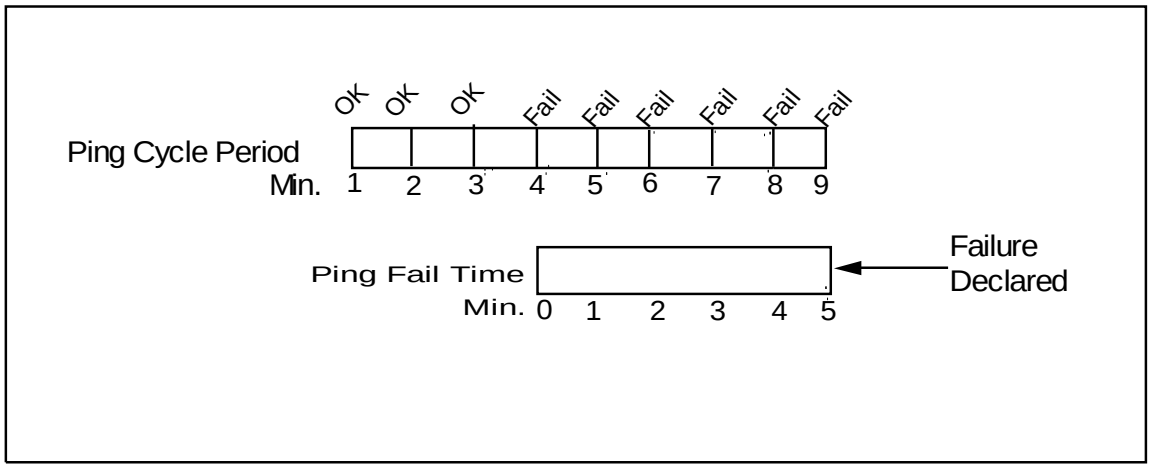
By referencing a control relay in the display and point fields, an event becomes a momentary relay time. Controls are mapped to Display 11, Points 1-4. See the Reference Section of this manual for display mapping information.

13.3.15 Setting System Timers

Timers		
	Value	Units
Cycle (1-120)	60	sec
Wait (1-12)	8	sec
Fail (1-120)	5	min
Sound (0-120)	6	sec
Channel (1-120)	2	min
Craft (0-120)	0	min
DCP (0-120)	30	sec
Tmd Tick (0-60)	0	min
PPP (0-120)	15	min
NTP Sync (0-120)	60	min
Proxy (0-120)	20	min
Web Timeout (0-120)	10	min
Web Refresh (5-120)	60	sec
LCD Delay (1-60)	2	sec

Submit Data

When a target fails to respond to a ping within the fail time period, a fault is declared



Default timer settings

The NetGuardian's System Timers allow you to control the rate of your pinging activity, time of speaker sounding, inactivity time for data ports, and discrete alarm detect time. Ping timer settings allow you to balance network traffic against alarm response times. Although you can change the values from their default settings, it is recommended that you use either the default settings or plan your settings so that there is no conflict among the timers. Specifically, the FAIL time should be set to several times the CYCLE time to allow multiple PINGs before a FAIL is declared. Likewise, the CYCLE time should be set to several times the wait time.

Hot Tip! The smaller the CYCLE number, the sooner you will find out about failures; however, you will increase traffic on your network.

1. From the **Edit** menu select **Timers**.
2. Set the **Cycle** time. This determines how often the NetGuardian will go through its list of ping targets and

attempts to reach them with an ICMP ping. Set the value between zero and 120 and set the units to either seconds or minutes. Default is 60 seconds.

3. Set the **Wait** time. The NetGuardian waits after sending a ping request before it determines that the target is unreachable. Set the value between zero and 12 and set the units to either seconds or minutes. Default is 8 seconds.
4. Set the **Fail** time. This determines the period of time over which, if a unit has not responded, it is considered failed. Set the value between zero and 120 and set the units to either seconds or minutes. Default is 5 minutes.
5. Set the **Sound** time. This determines how long the NetGuardian's speaker will sound when an alarm occurs or clears. The alarm condition will still be present after the speaker shuts off. The sound timer only affects the duration of the audible alarm annunciation. Set the value between zero and 120 and set the units to either seconds or minutes.
6. Set the **Channel** time. This determines the period of time over which, if there is no activity on the data ports designated as channel ports, it is considered failed. Set the value between zero and 120 and set the units to either seconds or minutes. Alarm activity is indicated in Display 11, Point 62. (See Appendix A, "Display Mapping.")
7. Set the **Craft** time. This determines the period of time over which, if the device connected through a port designated as a **craft** port doesn't reset the timer, an alarm will be triggered. Set between 0 and 120 (min or sec). Alarm activity is indicated in Display 11, Point 63. (See Appendix A, "Display Mapping.")
8. Set the **DCP** time. Set between 0–120 (sec or min). This determines the period of time over which, if the NetGuardian does not receive a DCP poll, to trigger an alarm. Once the alarm is triggered, then dial back-up may be enabled if a T/Mon pager profile is configured.
9. Set the **Timed Tick** between 0–60 minutes. This is a "keep alive or heartbeat" function that can be used by Masters who don't perform integrity checks. For example, if you entered 30, the NetGuardian would notify you every 30 minutes. See section "Setting Up Notification Methods" for paging information.
10. Set the **PPP** time. Set between 0–120 for onDemand mode.
11. Set the **NTP** Sync. Set between 0–120 (sec or min).

Note: The timer settings are accurate to ± one tick. This means that if a timer is set to one minute, it may actually respond anywhere from zero to two minutes. If your target time is one minute, then set the timer to 60 seconds so that it will respond anywhere from 59-61 seconds.

12. Set the **Proxy** time between 0-120 minutes. This indicates the length of time that has to pass before a proxy connection times-out from inactivity.
13. Set the **Web Edit Timeout** time between 5–120 minutes. This determines the period of time a Web edit page may be active without any activity. A logon is required if a Web edit timeout occurs. The default Web edit time is 10 mins.

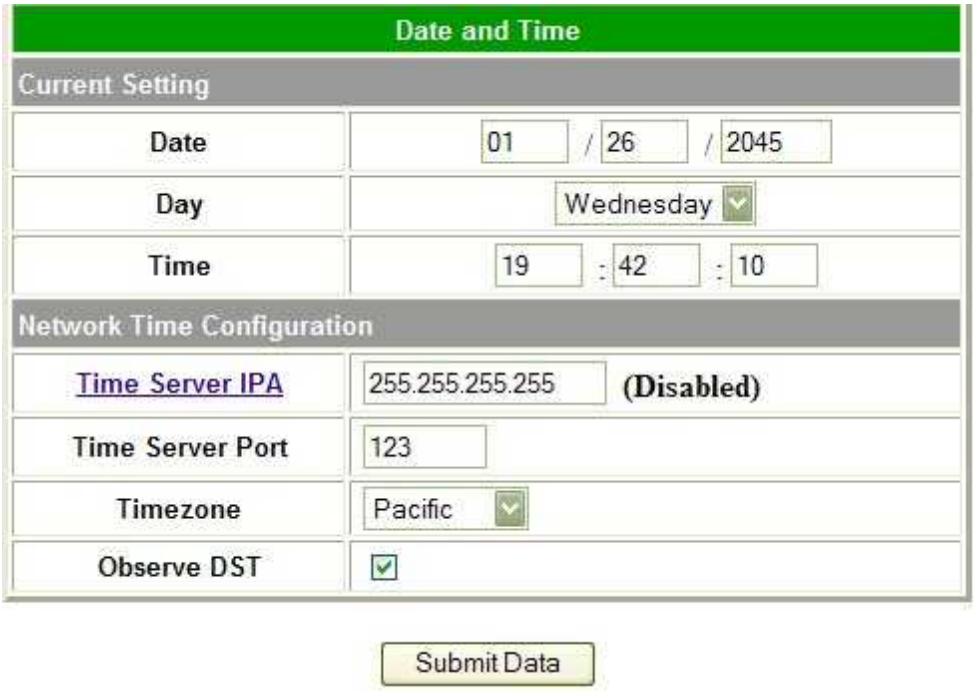
    Note: The time units are preset to minutes by default and cannot be changed.

14. Set the **Web Monitor Refresh** time between 5–120 seconds. This timer enables the user to specify how long the NetGuardian should wait before auto-refreshing a Monitor page to the Web browser. The default Web monitor refresh time is 60 seconds.

    Note: The time units are preset to seconds by default and cannot be changed.

15. Set the **LCD Delay** time between 1–60 seconds. This timer is used when you have set the LCD to "Point Mode." This time is how long you want the alarm to be displayed on the front panel LCD screen. The default is 2 seconds.
16. Set the **LCD Scroll** speed between 100 to 1000 milliseconds. This timer is used to configure how much time passes for the LCD to continue scrolling. The default is 600 milliseconds.

13.3.16 Setting the System Date and Time



The current date and time can be entered from the Date and Time screen or from an SNMP manager

The date is entered in the mm/dd/yyyy format and the time is entered in the hh:mm:ss format.

Hot Tip!

The date and time can also be set from an SNMP manager.

Use the following steps to manually set the system's time and date:

1. From the **Edit** menu, select **Date and Time**, see Figure 2.31.
2. Enter the appropriate date, the day of the week, and time.
3. Click **Submit Data** to save the data and time settings.

The date and time will need resetting following a power failure or reboot unless your NetGuardian is equipped with the real-time clock option or network time is enabled.

13.3.16.1 Network Time Protocol Support

Configure the Network Time Protocol feature in the Date and Time screen

Network Time Protocol support enables you to set a server to provide your NetGuardian the correct date and time, so you don't have to enter the information if your NetGuardian loses power or has to be reset to factory settings.

To enable Network Time Support:
1. From the **Edit** menu select **Date and Time.**
2. Click on the **Time Zone** drop-down menu and select the appropriate time zone.
3. Put a check next to **Observe DST** if you are in an area that observes daylight saving.
4. Enter the IP of the network time server in the **Time Server IPA** field.

Note: To disable NTP support, simply set the **Time Server IPA** to 255.255.255.255

6. Click **Submit Data** to save the date and time settings.

13.3.17 PPP Modes

Configure the PPP port settings in the Edit menu > PPP screen

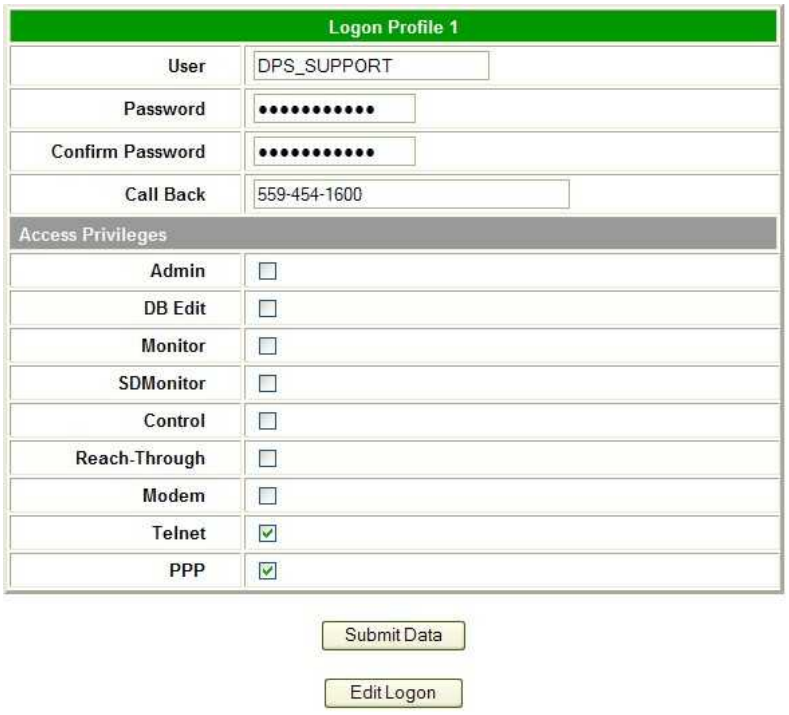
If the LAN connection to your remote sites fails, you can still keep in touch with your remote equipment by using the NetGuardian as a PPP (Point-to-Point Protocol) server via dial-up.

To configure the NetGuardian as a PPP Server:

1. Select **PPP** from the **Edit** menu.
2. In the **Server** section check the **Enable Server** (also known as Hosting Mode) box.
3. Set the IP address that is given to the guest dialing in. (This must be a valid and available IP address for the subnet on the LAN you will be connecting to, the same one the NetGuardian is connected to.)
4. Click **Submit Data** to save your PPP settings.

Edit the Modem settings for the PPP server in the Edit menu > Ports screen > Modem section

5. Select **Ports** from the **Edit** menu.
6. Scroll down to the **Modem** section. Make sure the **Ring Count** field is greater than 0.
7. In Answer Init String field type **&Q6**.
8. Click **Submit Data** to save your Modem changes.



Select PPP and Telnet access privileges in the Edit menu > Logon > Logon Profiles screen

9. Make sure the users who will need it have the access privilege to access the unit via Telnet. Select **Logon** in the **Edit** menu.

Hot Tip!

There can be up to 16 different user names and each one must have its own password.

10. Click the **Available** link or the user you want to have PPP and Telnet access privileges.
11. Under the **Access Privileges** section check the **PPP** and **Telnet** boxes.
12. Click **Submit Data** to save the configuration settings.
13. Select **Reboot** in **Edit** menu to reboot the NetGuardian. (See section "Rebooting the NetGuardian.")

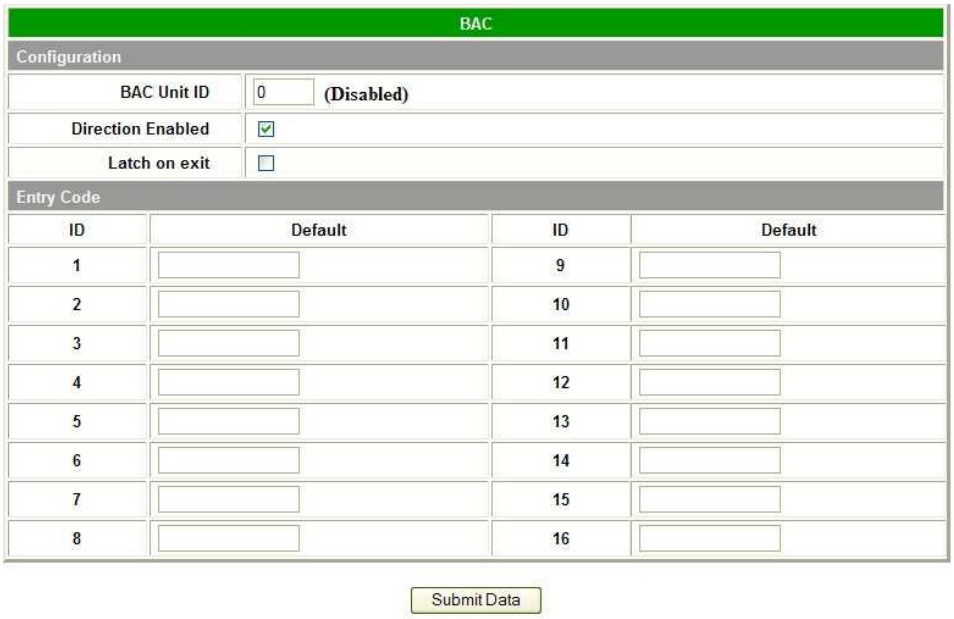
You also need to configure your remote terminal modem in order to access your NetGuardian by following these steps:

Windows 98 users: Set baud rate to **9600.**

Windows 2000, XP users: In **Modem Configuration General** tab uncheck **Enable modem error control** and **Enable compression.**

Mac OSX users: Use standard dial-in.

13.3.18 Building Access Control



Passwords entered in the NetGuardian will only remain valid until BAC provisioning information is downloaded from T/MonXM.

The Building Access Controller (BAC) option is only available for NetGuardian 420 builds with an RS-485 connection attached to an Entry Control Unit (ECU).

1. Enter the BAC unit ID number (This is the DCP address of the ECU. It must match the expansion address being polled by the master. Any range from 1-255 is acceptable or enter zero to disable the unit).

2. When **Direction** is enabled, users are required to enter a 1 for enter immediately following their password or a 4 for exit immediately following their password. For example, if the password is 4541600, and direction is enabled , users need to type in 45416001# to enter, or 45416004# to exit.

3. The Defaults column is where door passwords can be edited. These passwords are temporary passwords used primarily for turn up and test. A valid password is a combination of up to 14 digits. When a valid password is entered on the keypad, the NetGuardian will send a command to the Entry Control Unit (ECU) to operate the relay to energize the door strike.

Hot Tip!

Be sure to define the data port you are using for the ECU as an **ECU** type.

To configure Building Access on T/Mon, see your T/MonXM manual.

13.3.19 Configuring IP Cameras

The NetGuardian SiteMon G2 provides users with live streaming video of their remote sites. The direct pan-and-tilt features allows users to visually check the status of their sites from the convenience of their desktop. The NetGuardian allows your to view up to four cameras from the NetGuardian web interface.

To configure your camera settings:
1. From the **Edit** menu select **Camera**.
2. Enter the appropriate information in the **Name**, **Description**, **IP Address**, and **MAC Address** fields for each of your cameras.
   Note: See Section "Monitoring Camera Activity" for camera viewing options.
3. Click Submit Data to save your camera configuration settings.

View live streaming video of your remote sites via Web browser

Appropriate Web Browser Settings
In order to perform the pan-and-tilt functions of the camera, your Web browser must be set to check for newer versions of stored pages at every visit to the page.

The directions for checking for newer versions of stored pages may vary depending on what version of Windows you are running. The instructions below are relevant to Internet Explorer 5.5 and 6.0 only.

1. With the Web browser open (Internet Explorer version 5.5 or later), click on **Tools** and select **Internet Options** from the drop-down menu.
2. Click on the **Settings** button under the **Temporary Internet files** heading.
3. Click on the **Every visit to the page** button and click Ok.

13.3.20 Alarm Sync

Clicking on the Alarm Sync link from the Edit menu will re-synchronize all of the NetGuardian alarms. This command clears all alarms, so that a new notification is sent for all standing alarms. This allows you to easily test alarm connections during turnup without rebooting the NetGuardian unit. A warning prompt will appear, click **Ok** to continue or **Cancel** to exit without resynchronizing your alarms.

Click Ok to re-synchronize the NetGuardian alarms or Cancel to exit

13.3.21 Saving Changes or Resetting Factory Defaults

Your NetGuardian 420 comes equipped with Non Volatile RAM (NVRAM), which enables the retention of data in the event of power loss. You may use the NVRAM function from the web interface to either write your changes to the NetGuardian or revert to factory defaults.

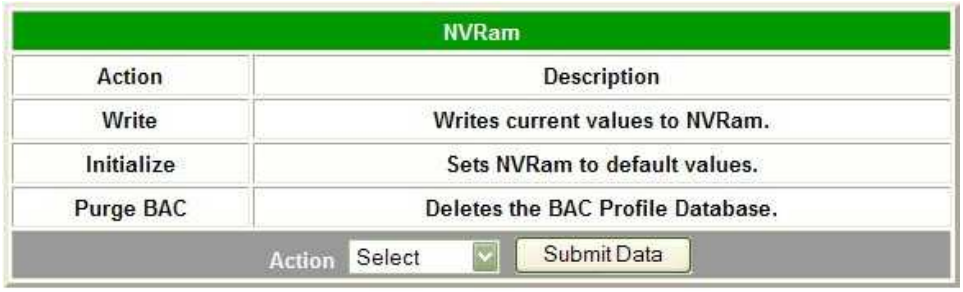
Some changes require a reboot of the NetGuardian to take effect, see Section "Rebooting the NetGuardian."

To access NVRAM:

1. From the **Edit** menu select **NVRAM**.
2. Select **Write** to cause the current data in RAM to be written to NVRAM and then verified.
3. Select **Initialize** to reload factory defaults into NVRAM.

DO NOT SELECT THIS OPTION UNLESS YOU WANT TO RE-CONFIGURE YOUR NETGUARDIAN.

4. Select **Purge BAC** to delete the Building Access Controller profile database downloaded from T/Mon XM.



NVRAM enables the NetGuardian to retain data even through a power loss

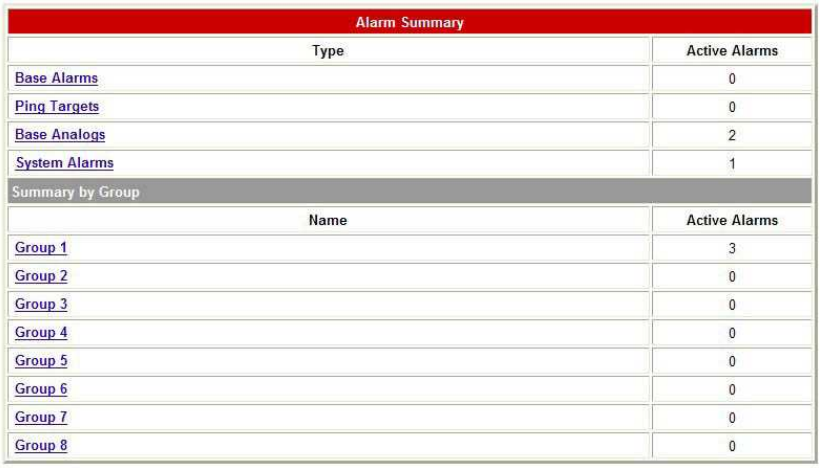
13.3.21.1 Rebooting the NetGuardian

Click on the **Reboot** link from the **Edit** menu to reboot the NetGuardian after writing all changes to NVRAM. Any changes to port settings require a reboot to take effect. The window footer will display the text **Reboot Needed** if a reboot is necessary to initiate changes.

13.4 Monitor Mode

From Monitor Mode, you can monitor all of the unit's alarms, analogs, ping targets, cameras, and issue controls. When you logon to the NetGuardian, it will be in Monitor Mode. To revert to Monitor Mode from Edit Mode, simply click the blue Monitor button.

13.4.1 Alarm Summary

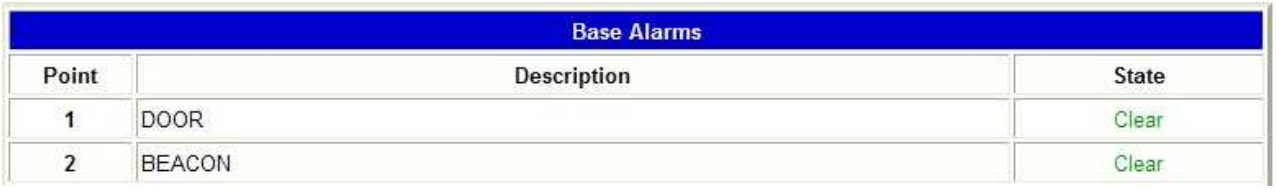


Alarm Summary	
Type	Active Alarms
Base Alarms	0
Ping Targets	0
Base Analogs	2
System Alarms	1
Summary by Group	
Name	Active Alarms
Group 1	3
Group 2	0
Group 3	0
Group 4	0
Group 5	0
Group 6	0
Group 7	0
Group 8	0

Entering Monitor Mode will bring you to the Alarm Summary Screen. From here, you can see the total number of active alarms, ping targets, analogs, and system alarms. You can also view alarms by point group. Click any of the links in the Alarm Summary to see details or use the navigation links on the left to browse your NetGuardian's alarms and resources.

13.4.2 Base Alarms

From the Base Alarms screen, you can view the state of your NetGuardian's 20 base alarms.



Base Alarms		
Point	Description	State
1	DOOR	Clear
2	BEACON	Clear

If you added alarms to point groups, the state field will display the appropriate set or clear messages. If you're ever unsure of the set or clear messages, green font will always indicate a cleared alarm, red will always indicate a set alarm.

13.4.3 Ping Targets

You can monitor your NetGuardian's 32 ping targets from the **Monitor > Ping Targets** screen.

Ping Targets		
Point	Description	State
1		Clear

If you added your ping targets to point groups, the state field will display the appropriate set or clear messages. If you're ever unsure of the set or clear messages, green font will always indicate a cleared alarm, red will always indicate a set alarm.

13.4.4 Base Analogs

The **Monitor** menu > **Analogs** screen provides a description of each analog channel, the current reading, the units being read, and alarm conditions (major under, minor under, major over, minor over) according to your analog settings.

Base Analogs							
Chn	Description	Reading	Units	MjU	MnU	MnO	MjO
5	INPUT VOLTAGE A	-49.3702	VDC				
7	INT TEMPERATURE	80.6204	iF				
8	EXT TEMPERATURE	51.3041	eF			x	x

13.4.5 System Alarms

The System Alarms link will show you the state of your NetGuardian's internal alarms.

System Alarms		
Point	Description	State
17	Timed Tick	Clear
18	Exp.Module Callout	Clear
19	Network Time Server	Clear
20	Accumulation Event	Clear
21	Duplicate IP Address	Clear

If you added alarms to point groups, the state field will display the appropriate set or clear messages. However, in the state field, green font will always indicate a cleared alarm, red will always indicate a set alarm.

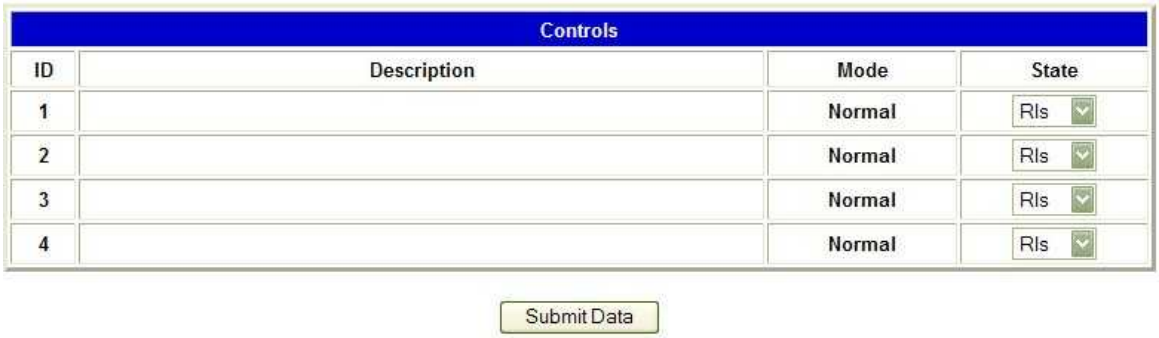
13.4.6 Accum Timer

Clicking on **Accum. Timer** will take you to the Accumulation Timer. From here, you can see how many times an alarm (configured from the Accum Timer field in Edit Mode) has occurred in a set period of time.

Accum. Timer	
Display Reference	0
Point Reference	0
Point Description	Undefined
Point Status	-
Event Threshold	00:00:00 (dd:hh:mm)
Accumulated Time	00:00:00 (dd:hh:mm)
Accumulated Since	01-Jan-2001 12:00

13.4.7 Controls

Selecting **Controls** from the Monitor Mode navigation menu gives the user access to the unit's control relays



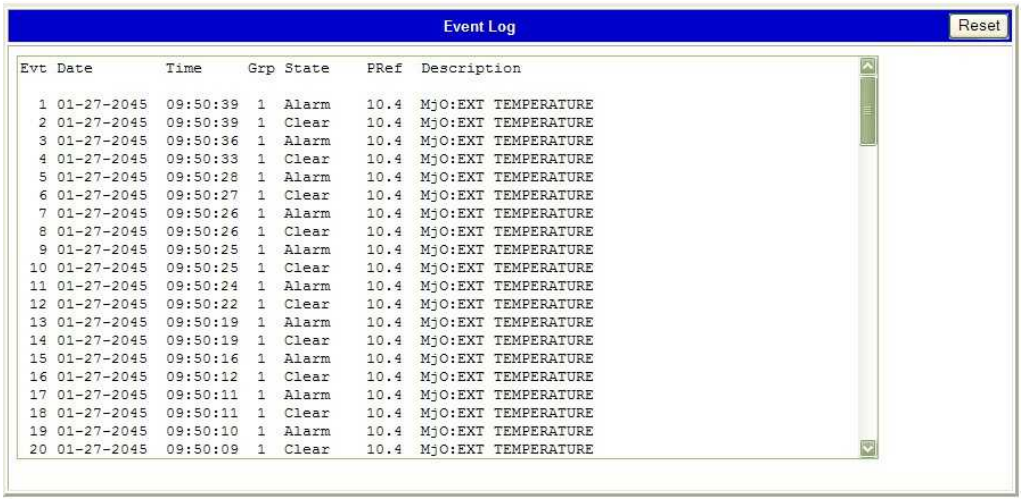
To operate controls:

1. Under the **State** field, choose a command (Opr - operate, Rls - release, or Mom - momentary).
2. Click **Submit Data** to issue the control.

The control relay's normal state - open or closed - is determined by a PCB jumper. Operating a control thus changes the normal state of the relay (energizes it) until it is released (de-energized). By default, the momentary command energizes the relay for approximately one second before it is released again. Use the event qualifiers to extend the momentary period.

13.4.8 Event Log

To view a log of alarm events, click **Event Log** in the Monitor Menu Navigation frame.


Event Log
Reset
Evt Date Time Grp State PRef Description
1 01-27-2045 09:50:39 1 Alarm 10.4 MjO:EXT TEMPERATURE
2 01-27-2045 09:50:39 1 Clear 10.4 MjO:EXT TEMPERATURE
3 01-27-2045 09:50:36 1 Alarm 10.4 MjO:EXT TEMPERATURE
4 01-27-2045 09:50:33 1 Clear 10.4 MjO:EXT TEMPERATURE
5 01-27-2045 09:50:28 1 Alarm 10.4 MjO:EXT TEMPERATURE
6 01-27-2045 09:50:27 1 Clear 10.4 MjO:EXT TEMPERATURE
7 01-27-2045 09:50:26 1 Alarm 10.4 MjO:EXT TEMPERATURE
8 01-27-2045 09:50:26 1 Clear 10.4 MjO:EXT TEMPERATURE
9 01-27-2045 09:50:25 1 Alarm 10.4 MjO:EXT TEMPERATURE
10 01-27-2045 09:50:25 1 Clear 10.4 MjO:EXT TEMPERATURE
11 01-27-2045 09:50:24 1 Alarm 10.4 MjO:EXT TEMPERATURE
12 01-27-2045 09:50:22 1 Clear 10.4 MjO:EXT TEMPERATURE
13 01-27-2045 09:50:19 1 Alarm 10.4 MjO:EXT TEMPERATURE
14 01-27-2045 09:50:19 1 Clear 10.4 MjO:EXT TEMPERATURE
15 01-27-2045 09:50:16 1 Alarm 10.4 MjO:EXT TEMPERATURE
16 01-27-2045 09:50:12 1 Clear 10.4 MjO:EXT TEMPERATURE
17 01-27-2045 09:50:11 1 Alarm 10.4 MjO:EXT TEMPERATURE
18 01-27-2045 09:50:11 1 Clear 10.4 MjO:EXT TEMPERATURE
19 01-27-2045 09:50:10 1 Alarm 10.4 MjO:EXT TEMPERATURE
20 01-27-2045 09:50:09 1 Clear 10.4 MjO:EXT TEMPERATURE

The NetGuardian's Event Log allows the NetGuardian to post and monitor up to 100 events including power up, base and system alarms, ping alarms, analog alarms, and controls. Posted events for the various alarms include both alarm and clear status. All information in the event log will be erased upon reboot or a power failure.

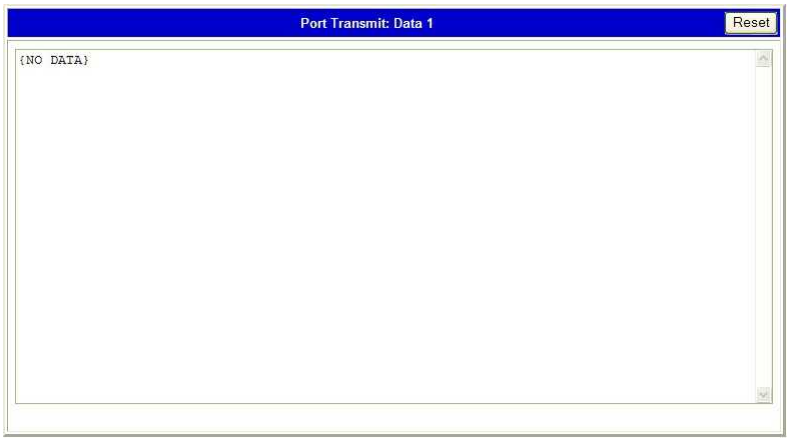
Event Log Field	Description
Evt	Event number (1-100)
Date	Date the event occurred
Time	Time the event occurred
St	State of the event (A=alarm, C=clear)
Pref	Point reference.
Description	User defined description of the event as entered in the alarm point and relay description fields

Event Logging window field descriptions

13.4.9 Monitoring Port Activity

To view the data being received by the connected equipment, select the data port number from the Monitor menu > Port Receive drop-down menu

The **Port Transmit** and **Port Receive** screens provide live status information for the NetGuardian's 4 data ports by displaying transmit or receive activity in ASCII for the selected port. See "ASCII Conversion" in the Reference Section of this manual for specific ASCII symbol conversion.



The Port Transmit screen displays activity for the selected port

Hot Tip!

Use the NetGuardian's `CHAN` feature to analyze bi-directional communication between two device in real time, see section "Data Port Types."

14 Reference Section

14.1 Display Mapping

Port	Address	Display	Points	Description	Set	Clear
99	1	1	1-20	Discrete Alarms 1-20	8001-8020	9001-9020
99	1	2	1-32	Ping Table	8065-8096	9065-9096
99	1	3	1-4	Analog Channel 1**	8129-8132	9129-9132
99	1	4	1-4	Analog Channel 2**	8193-8196	9193-9196
99	1	5	1-4	Analog Channel 3**	8257-8260	9257-9260
99	1	6	1-4	Analog Channel 4**	8321-8324	9321-9324
99	1	7	1-4	Analog Channel 5**	8385-8388	9385-9388
99	1	8	1-4	Analog Channel 6**	8449-8452	9449-9452
99	1	11	1-4	Control Relays	8641-8644	9641-9644
99	1	11	17-63	System Alarms	8657-8704	9657-9704
99	1	12	1-64	NetGuardian Expansion 1 Alarms 1-64	6001-6064	7001-7064
99	1	13	1-8	NetGuardian Expansion 1 Relays 1-8	6065-6072	7065-7072
99	1	14	1-64	NetGuardian Expansion 2 Alarms 1-64	6129-6193	7129-7193
99	1	15	1-8	NetGuardian Expansion 2 Relays 1-8	6193-6200	7193-7200
99	1	16	1-64	NetGuardian Expansion 3 Alarms 1-64	6257-6321	7257-7321
99	1	17	1-8	NetGuardian Expansion 3 Relays 1-8	6321-6328	7321-7328

Display descriptions and SNMP Trap numbers for the NetGuardian

* The TRAP number ranges shown correspond to the point range of each display. For example, the SNMP Trap "Set" number for alarm 1 (in Display 1) is 8001, "Set" for alarm 2 is 8002, "Set" for alarm 3 is 8003, etc.

** The TRAP number descriptions for the Analog channels (1-8) are in the following order: minor under, minor over, major under, and major over. For example, for Analog channel 1, the "Set" number for minor under is 8129, minor over is 8130, major under is 8131, and major over is 8132.

14.1.1 System Alarms Display Map

Display	Points	Alarm Point	Description	Solution
11	17	Timed Tick	Toggles state at constant rate as configured by the Timed Tick timer variable. Useful in testing integrity of SNMP trap alarm reporting.	To turn the feature off, set the Timed Tick timer to 0.
	18	Exp. Module Callout	Alarm is triggered whenever an alarm point from an Entry Control Unit (ECU) is collected. A notification event may be associated with the alarm to force a call out or trap.	Disable Building Access Control (BAC) by setting the BAC Unit ID to 0. If Building Access is being used, then investigate the ECU alarm source or don't associate notification with the alarm event.
	19	Network Time Server	Communication with Network Time Server has failed.	Try pinging the Network Time Server's IP Address as it is configured. If the ping test is successful, then check the port setting and verify the port is not being blocked on your network.
	20	Accumulation Event	An alarm has been standing for the time configured under Accum. Timer. The Accumulation timer enables you to monitor how long an alarm has been standing despite system reboots. Only the user may reset the accumulated time, a reboot will not.	To turn off the feature, under Accum. Timer, set the display and point reference to 0.
	21	Duplicate IP Address	The unit has detected another node with the same IP Address.	Unplug the LAN cable and contact your network administrator. Your network and the unit will most likely behave incorrectly. After assigning a correct IP Address, reboot the unit to clear the System alarm.
	33	Power Up	The unit has just come-online. The set alarm condition is followed immediately by a clear alarm condition.	Seeing this alarm is normal if the unit is powering up.
	36	Lost Provisioning	The internal NVRAM may be damaged. The unit is using default configuration settings.	Use Web to configure unit. Power cycle to see if alarm goes away. May require RMA.

System Alarms Descriptions

Note: Table 14.1.1.A. continues on following pages.

Display	Points	Alarm Point	Description	Solution
11	37	DCP Poller Inactive	The unit has not seen a poll from the Master for the time specified by the DCP Timer setting.	If DCP responder is not being used, then set the DCP Unit ID to 0. Otherwise, try increasing the DCP timer setting under timers, or check how long it takes to cycle through the current polling chain on the Master system.
	38	NET1 not active	The Net1 LAN port is down.	Check LAN cable. Ping to and from the unit. (If not using Net1 or Net2, set IP, Subnet and Gateway to 255's)
	39	NET2 not active	The Net2 LAN port is down.	
	40	LNK Alarm	No network connection detected	
	41	Modem not responding	An error has been detected during modem initialization. The modem did not respond to the initialization string.	Remove configured modem initialization string, then power cycle the unit. If alarm persists, try resetting the Modem port from the TTY interface, or contact DPS for possible RMA.
	42	No Dial Tone	During dial-out attempt, the unit did not detect a dial tone.	Check the integrity of the phone line and cable.
	43	SNMP Trap not Sent	SNMP trap address is not defined and an SNMP trap event occurred.	Define the IP Address where you would like to send SNMP trap events, or configure the event not to trap.
	44	Pager Queue Overflow	Over 250 events are currently queued in the pager queued and are still trying to report.	Check for failed notification events that may be filling up the pager queue. There may be a configuration or communication problem with the notification events.
	45	Notification failed	A notification event, like a page or email, was unsuccessful.	Use RPT filter debug to help diagnose notification problems.
	46	Craft RcvQ full	The Craft port received more data than it was able to process.	Disconnect whatever device is connected to the craft serial port. This alarm should not occur.
	47	Modem RcvQ full	The modem port received more data than it was able to process.	Check what is connecting to the NetGuardian. This alarm should not occur.
	48	Serial 1 RcvQ full	Serial port 1 (or appropriate serial port number) receiver filled with 8 K of data (4 K if BAC active).	Check proxy connection. The serial port data may not be getting collected as expected.
	49	Serial 2 RcvQ full		
	50	Serial 3 RcvQ full		
	51	Serial 4 RcvQ full		
	52	Serial 5 RcvQ full		
	53	Serial 6 RcvQ full		
	54	Serial 7 RcvQ full		
	55	Serial 8 RcvQ full		

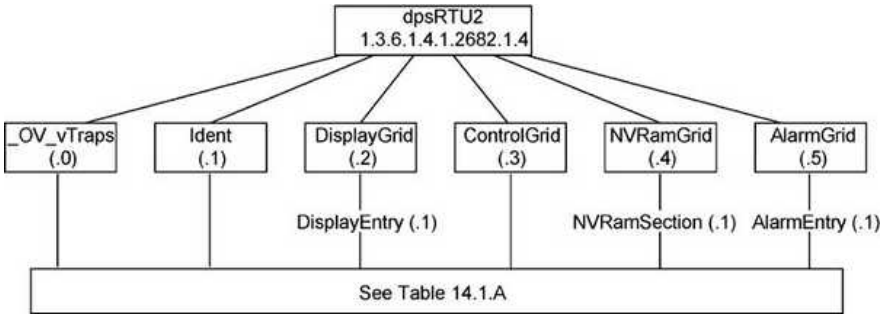
System Alarms Descriptions (continued)

Display	Points	Alarm Point	Description	Solution
11	56	NetGuardian DX 1 fail	NGDdx 1 Fail (Expansion shelf 1 communication link failure)	Under Ports > Options, verify the number of configured NGDdx units. Use EXP filter debug and port LEDs to help diagnose the problem. Use DB9M to DB9M with null crossover for cabling. Verify the DIP addressing on the back of the NGDdx unit.
	57	NetGuardian DX 2 fail	NGDdx 2 Fail (Expansion shelf 2 communication link failure)	
	58	NetGuardian DX 3 fail	NGDdx 3 Fail (Expansion shelf 3 communication link failure)	
	59	GLD 1 fail	GLD address 1 is failed.	Connect just GLD unit 1 and attempt to poll. Verify GLD is connected to data port 8 and the hardware is RS485, not RS232.
	60	GLD 2 fail	GLD address 2 is failed.	Verify the GLD unit addressing, and test GLD units individually on the GLD communication bus.
	61	GLD 3+ fail	One or more GLD units addressed 3 through 12 may be failed.	Reduce the number of connected GLD units to determine which unit may be causing the link to fail.
	62	Chan. Port Timeout	Chan. Port has not forwarded any traffic in the time specified by the Channel Timeout Timer. The channel feature forwards data between two ports so the NG may be used to analyze serial traffic using CHAN filter debug.	Change the data port type to OFF, or set the Channel Timer to a different setting.
	63	Craft Timeout	The Craft Timeout Timer has not been reset in the specified time. This feature is designed so other machines may keep the TTY link active. If the TTY interface becomes unavailable to the machine, then the Craft Timeout alarm is set.	Change the Craft Timeout Timer to 0 to disable the feature.
	64	Event Que Full	The Event Que is filled with more than 500 uncollected events.	Enable DCP timestamp polling on the master so events are collected, or reboot the system to clear the alarm.

System Alarms Descriptions (continued)

14.2 SNMP Manager Functions

The SNMP Manager allows the user to view alarm status, set date/time, issue controls, and perform a resync. The display and tables below outline the MIB object identifiers. Table B.1 begins with dpsRTU; however, the MIB object identifier tree has several levels above it. The full English name is as follows: root.iso.org.dod.internet.private. enterprises.dps-Inc.dpsAlarmControl.dpsRTU. Therefore, dpsRTU's full object identifier is 1.3.6.1.4.1.2682.1.4. Each level beyond dpsRTU adds another object identifying number. For example, the object identifier of the Display portion of the Control Grid is 1.3.6.1.4.1.2682.1.4.3.3 because the object identifier of dpsRTU is 1.3.6.1.4.1.2682.1.4 + the Control Grid (.3) + the Display (.3).



Tbl. B1 (O.)_OV_Traps points
_OV_vTraps (1.3.6.1.4.1.2682.1.4.0)
PointSet (.20)
PointClr (.21)
SumPSet (.101)
SumPClr (.102)
ComFailed (.103)
ComRestored (.014)
P0001Set (.10001) through P0064Set (.10064)
P0001Clr (.20001) through P0064Clr (.20064)

Tbl. B2 (.1) Identity points
Ident (1.3.6.1.4.1.2682.1.4.1)
Manufacturer (.1)
Model (.2)
Firmware Version (.3)
DateTime (.4)
ResyncReq (.5)*
* Must be set to "1" to perform the resync request which will resend TRAPs for any standing alarm.

Tbl. B3 (.2) DisplayGrid points
DisplayEntry (1.3.6.1.4.1.2682.1.4.2.1)
Port (.1)
Address (.2)
Display (.3)
DispDesc (.4)*
PntMap (.5)*

Tbl. B3 (.3) ControlGrid points
ControlGrid (1.3.6.1.4.1.2682.1.4.3)
Port (.1)
Address (.2)
Display (.3)
Point (.4)
Action (.5)

Tbl. B5 (.5) AlarmEntry points
AlarmEntry (1.3.6.4.1.2682.1.4.5.1)
Aport (.1)
AAddress (.2)
ADisplay (.3)
APoint (.4)
APntDesc (.5)*
AState (.6)
* For specific alarm points, see Table B6

14.3 SNMP Granular Trap Packets

Tables 14.3.A and 14.3.B provide a list of the information contained in the SNMP Trap packets sent by the NetGuardian.

SNMP Trap managers can use one of two methods to get alarm information:
1. Granular traps (not necessary to define point descriptions for the NetGuardian)
or
2. The SNMP manager reads the description from the Trap.

UDP Header	Description
1238	Source port
162	Destination port
303	Length
0xBAB0	Checksum

UDP Headers and descriptions

SNMP Header	Description
0	Version
Public	Request
Trap	Request
1.3.6.1.4.1.2682.1.4	Enterprise
126.10.230.181	Agent address
Enterprise Specific	Generic Trap
8001	Specific Trap
617077	Time stamp
1.3.7.1.2.1.1.1.0	Object
NetGuardian 216 v1.0K	Value
1.3.6.1.2.1.1.6.0	Object
1-800-622-3314	Value
1.3.6.1.4.1.2682.1.4.4.1.0	Object
01-02-1995 05:08:27.760	Value
1.3.6.1.4.1.2682.1.4.5.1.1.99.1.1.1	Object
99	Value
1.3.6.1.4.1.2682.1.4.5.1.2.99.1.1.1	Object
1	Value
1.3.6.1.4.1.2682.1.4.5.1.3.99.1.1.1	Object
1	Value
1.3.6.1.4.1.2682.1.4.5.1.4.99.1.1.1	Object
1	Value
1.3.6.1.4.1.2682.1.4.5.1.5.99.1.1.1	Object
Rectifier Failure	Value
1.3.6.1.4.1.2682.1.4.5.1.6.99.1.1.1	Object
Alarm	Value

14.4 Trap SNMP Logic

NET1	NET2	Trap Dest.	Result
Subnet 1 & Gateway	Not Defined	Subnet 3	Trap goes out NET1's Gateway
Subnet 1 & Gateway	Subnet 2, No Gateway	Subnet 3	Trap goes out NET1's Gateway
Subnet 1 & Gateway	Subnet 2 & Gateway	Subnet 3	Trap goes out NET2's Gateway
Subnet 1 & Gateway	Subnet 2 & Gateway	Subnet 2	Trap goes out NET2
Subnet 1 & Gateway	Subnet 2 & Gateway	Subnet 1	Trap goes out NET1
Subnet 1, No Gateway	Subnet 2 & Gateway	Subnet 1	Trap goes out NET1
Subnet 1, No Gateway	Subnet 2 & Gateway	Subnet 2	Trap goes out NET2
Subnet 1, No Gateway	Subnet 2 & Gateway	Subnet 3	Trap goes out NET2

Trap SNMP Logic

14.5 ASCII Conversion

The information contained in Table D.1 is a list of ASCII symbols and their meanings. Refer to the bulleted list below to interpret the ASCII data transmitted or received through the data ports. Port transmit and receive activity can be viewed from the Web Browser Interface.

- Printable ASCII characters will appear as ASCII.
- Non-printable ASCII characters will appear as labels surrounded by { } brackets (e.g. {NUL}).
- Non-ASCII characters will appear as hexadecimal surrounded by [ ] brackets (e.g. [FF]).
- A received BREAK will appear as <BRK>.

Abbreviation	Description	Abbreviation	Description
NUL	Null	DLE	Data Link Escape
SOH	Start of Heading	DC	Device Control
STX	Start of Text	NAK	Negative Acknowledge
ETX	End of Text	SYN	Synchronous Idle
EOT	End of Transmission	ETB	End of Transmission Block
ENQ	Enquiry	CAN	Cancel
ACK	Acknowledge	EM	End of Medium
BEL	Bell	SUB	Substitute
BS	Backspace	ESC	Escape
HT	Horizontal Tabulation	FS	File Separator
LF	Line Feed	GS	Group Separator
VT	Vertical Tabulation	RS	Record Separator
FF	Form Feed	US	Unit Separator
CR	Carriage Return	SP	Space (blank)
SO	Shift Out	DEL	Delete
SI	Shift In	BRK	Break Received

ASCII symbols

14.6 RADIUS Dictionary File (Available on Resource Disk)

```
# -*- text -*-
#
# dictionary.dps
#
#       DPS Telecom, Inc
#       For assistance or support, please contact support@dpstele.com
#                       v1.0 Released - 1/23/09 (CBH/DPS)

VENDOR          DPS                     2682

#
# Standard attribute for NetGuardian RTU.
# All values are integer with 1 = True, 0 = False.
# If attribure does not exist in Access-Accept packet, default value will be 0.
#
BEGIN-VENDOR    DPS

ATTRIBUTE   dps-admin                   1       integer
ATTRIBUTE   dps-edit                    2       integer
ATTRIBUTE   dps-monitor                 3       integer
ATTRIBUTE   dps-SD-monitor              4       integer
#To allow monitor of data port buffer/activity
ATTRIBUTE   dps-reach-through           5       integer
#To allow proxy to serial ports via TTY interface
ATTRIBUTE   dps-telnet                  6       integer
#To allow telnet in and out of NetGuardian
ATTRIBUTE   dps-control                 7       integer
#To allow manipulation of dry contact relay outputs
ATTRIBUTE   dps-modem                   8       integer
#To allow dial in and out of NetGuardian
ATTRIBUTE   dps-ppp                     9       integer
#To allow this user PPP (inbound) access to the NetGuardian

END-VENDOR      DPS
```

14.7 DNP3 Configuration / Interoperability Guide

14.7.1 DNP v3.0 Device Profile

The following table provides a "Device Profile Document" in the standard format defined in the DNP 3.0 Subset Definitions Document. While it is referred to in the DNP 3.0 Subset Definitions as a "Document," it is in fact a table, and only a component of a total interoperability guide.

<table>
<tr><td colspan="2">DNP V3.0
DEVICE PROFILE DOCUMENT
(Also see the DNP 3.0 Implementation Table in Section 4.6.2)</td></tr>
<tr><td colspan="2">Vendor Name: DPS Telecom Inc.</td></tr>
<tr><td colspan="2">Device Name: NetGuardian 420</td></tr>
<tr><td>Highest DNP Level Supported:

For Requests: Level 3

For Responses: Level 3</td><td>Device Function:

☐ Master

☒ Slave</td></tr>
<tr><td colspan="2">Notable objects, functions, and/or qualifiers supported in addition to the Highest DNP Levels Supported (the complete list is described in the attached table):

The read function code for Object 50 (Time and Date), variation 1, is supported.</td></tr>
<tr><td>Maximum Data Link Frame Size (octets):

Transmitted: 292
Received: 292</td><td>Maximum Application Fragment Size (octets):

Transmitted: 512
Received: 512</td></tr>
<tr><td>Maximum Data Link Re-tries:

☐ None
☒ Fixed (3)</td><td>Maximum Application Layer Re-tries:

☒ None
☐ Configurable</td></tr>
<tr><td colspan="2">Requires Data Link Layer Re-tries:

Fixed (3)
☐ Always
☐ Sometimes</td></tr>
</table>

Requires Application Layer Confirmation:

- ☐ Never
- ☐ Always
- ☐ When reporting Event Data (Slave devices only)
- ☒ **When sending multi-fragment responses (Slave devices only)**
- ☐ Sometimes

DNP V3.0

DEVICE PROFILE DOCUMENT
(Also see the DNP 3.0 Implementation Table in Section 4.6.2)

Timeouts while waiting for:

Data Link Confirmation:	**Fixed at 2s**
Complete Appl. Fragment:	**None**
Application Confirm:	**Fixed at 10s**
Complete Appl. Response:	**None**
Other:	**Transmission Delay, 0**

Sends/Executes Control Operations:

WRITE Binary Outputs: **Never**
SELECT/OPERATE: **Never**
DIRECT OPERATE: **Always**
DIRECT OPERATE - NO ACK: **Always**

Count > 1: **Never**
Pulse On: **Never**
Pulse Off: **Never**
Latch On: **Always**
Latch Off: **Always**

Queue: **Never**
Clear Queue: **Never**

Reports Binary Input Change Events when no specific variation requested:

- ☒ **Never**
- ☐ Only time-tagged
- ☐ Only non-time-tagged

Reports time-tagged Binary Input Change Events when no specific variation requested:

- ☒ **Never**
- ☐ Binary Input Change With Time
- ☐ Binary Input Change with Relative Time

Sends Unsolicited Responses

- ☒ **Never**
- ☐ Only certain objects
- ☐ Sometimes (attach explanation)
- ☐ ENABLE/DISABLE UNSOLICITED Function codes supported

Sends Static Data in Unsolicited Responses:

- ☒ **Never**
- ☐ When Device Restarts
- ☐ When Status Flags Change

Default Counter Object/Variation:	Counters Roll Over at:
☒ **No Counters Reported** ☐ Default Object	☒ **No Counters Reported** ☐ Configurable (attach explanation) ☐ 16 Bits ☐ 32 Bits ☐ Other Value: ____ ☐ Point-by-point list attached

DNP V3.0

DEVICE PROFILE DOCUMENT
(Also see the DNP 3.0 Implementation Table in Section 4.6.2)

Sends Multi-Fragment Responses:
No
Yes

Sequential File Transfer Support: **No**
Append File Mode: **No**
Custom Status Code Strings: **No**
Permissions Field: **No**
File Events Assigned to Class: **No**
File Events Send Immediately: **No**
Multiple Blocks in a Fragment: **No**
Max Number of Files Open: **0**

14.7.2 DNP V3.0 Implementation Table

The following table identifies which object variations, function codes, and qualifiers the NetGuardian 420 supports in both request messages and in response messages. For static (non-change-event) objects, request send with qualifiers 00, 01, 06, 07, or 08 will be responded with qualifiers 00 or 01.

OBJECT			**REQUEST** (Library will parse)		**RESPONSE** (Library will respond with)	
Object Number	**Variation Number**	**Description**	**Function Codes (dec)**	**Qualifiers Codes (hex)**	**Function Codes (dec)**	**Qualifiers Codes (hex)**
1	1	Binary Input	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129 (response)	00, 01 (start-stop)
10	2	Binary Output Status	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129 (response)	00, 01 (start-stop)
12	1	Control Relay Output Block	5 (direct op) 6 (dir. op, noack)	17, 28 (index)	129 (response)	echo of request
30	3	32-Bit Analog Input Without Flag	1 (read)	00, 01 (start-stop) 06 (no range, or all)	129 (response)	00, 01 (start-stop)
50	1	Time and Date	1 (read)	07 (limited qty = 1)	129 (response)	07 (limited qty = 1)
			2 (write)	07 (limited qty = 1)		
60	1	Class 0 Data	1 (read)	06 (no range, or all)		
60	2	Class 1 Data	1 (read)	06 (no range, or all)		
60	3	Class 2 Data	1 (read)	06 (no range, or all)		
60	4	Class 3 Data	1 (read)	06 (no range, or all)		

14.7.3 DNP V3.0 Point List

The tables below identify all the default data points provided by the NetGuardian 420.

Obj 02 Var 02 - Binary Input Change with TIme		
Point Index	**Description/Points**	**Class**
0-19	Discrete Alarms 1 - 20	1
20-51	Ping Targets 1-32	1
52-99	System Alarms 17-64	1
100-163	DX1 Discretes 1-64	1
164-227	DX2 Discretes 1-64	1
228-291	DX3 Discretes 1-64	1
292-295	Controls 1-4	1
296-303	DX1 Controls 1-8	1
304-311	DX2 Controls 1-8	1
312-319	DX3 Controls 1-8	1
320-323	Analog1 1-4	1
324-327	Analog2 1-4	1
328-331	Analog3 1-4	1
332-335	Analog4 1-4	1
336-339	Analog5 1-4	1
340-343	Analog6 1-4	1
344-347	Analog7 1-4	1
348-351	Analog8 1-4	1
352-355	DX1 Analog1 1-4	1
356-359	DX1 Analog2 1-4	1
360-363	DX1 Analog3 1-4	1
364-367	DX1 Analog4 1-4	1
368-371	DX1 Analog5 1-4	1
372-375	DX1 Analog6 1-4	1
376-379	DX1 Analog7 1-4	1
380-383	DX1 Analog8 1-4	1
384-387	DX2 Analog1 1-4	1

388-391	DX2 Analog2 1-4	1
392-395	DX2 Analog3 1-4	1
396-399	DX2 Analog4 1-4	1
400-403	DX2 Analog5 1-4	1
404-407	DX2 Analog6 1-4	1
408-411	DX2 Analog7 1-4	1
412-415	DX2 Analog8 1-4	1
416-419	DX3 Analog1 1-4	1
420-423	DX3 Analog2 1-4	1
424-427	DX3 Analog3 1-4	1
428-431	DX3 Analog4 1-4	1
432-435	DX3 Analog5 1-4	1
436-439	DX3 Analog6 1-4	1
440-443	DX3 Analog7 1-4	1
444-447	DX3 Analog8 1-4	1

Analog Inputs

The following table lists Analog Inputs (Object 30). It is important to note that Analog Inputs, Analog Output Control Blocks, and Analog Output Statuses are transmitted through DNP as signed numbers. **Note:** Points 14-29 are used for DX 2 and DX 3 on units that **DO NOT** support D-Wire. For units that do support D-Wire, only 1 DX is supported (points 6-13), and points 14-29 are reserved for D-Wire.

Analog Inputs Static Variation: Obj 30 Var 03 - 32-Bit analog w/o flag Request function codes supported: 1 (read)			
Point ID	**Description**	**Default Unit**	**Class**
0	Analog Channel 1	Voltage (VDC)	3
1	Analog Channel 2	Voltage (VDC)	3
2	Analog Channel 3	Voltage (VDC)	3
3	Analog Channel 4	Voltage (VDC)	3
4	Analog Channel 5	Voltage (VDC)	3
5	Analog Channel 6	Voltage (VDC)	3
6	Analog Channel 7	Voltage (VDC)	3
7	Analog Channel 8	Voltage (VDC)	3
8	DX 1 Analog Channel 1	Voltage (VDC)	3
9	DX 1 Analog Channel 2	Voltage (VDC)	3

10	DX 1 Analog Channel 3	Voltage (VDC)	3
11	DX 1 Analog Channel 4	Voltage (VDC)	3
12	DX 1 Analog Channel 5	Voltage (VDC)	3
13	DX 1 Analog Channel 6	Voltage (VDC)	3
14	DX 1 Analog Channel 7	Voltage (VDC)	3
15	DX 1 Analog Channel 8	Voltage (VDC)	3
16	DX 2 Analog Channel 1 (or D-Wire 1 for unit with D-Wire support)	Voltage (VDC)	3
17	DX 2 Analog Channel 2 (or D-Wire 2 for unit with D-Wire support)	Voltage (VDC)	3
18	DX 2 Analog Channel 3 (or D-Wire 3 for unit with D-Wire support)	Voltage (VDC)	3
19	DX 2 Analog Channel 4 (or D-Wire 4 for unit with D-Wire support)	Voltage (VDC)	3
20	DX 2 Analog Channel 5 (or D-Wire 5 for unit with D-Wire support)	Voltage (VDC)	3
21	DX 2 Analog Channel 6 (or D-Wire 6 for unit with D-Wire support)	Voltage (VDC)	3
22	DX 2 Analog Channel 7 (or D-Wire 7 for unit with D-Wire support)	Voltage (VDC)	3
23	DX 2 Analog Channel 8 (or D-Wire 8 for unit with D-Wire support)	Voltage (VDC)	3
24	DX 3 Analog Channel 1 (or D-Wire 9 for unit with D-Wire support)	Voltage (VDC)	3
25	DX 3 Analog Channel 2 (or D-Wire 10 for unit with D-Wire support)	Voltage (VDC)	3
26	DX 3 Analog Channel 3 (or D-Wire 11 for unit with D-Wire support)	Voltage (VDC)	3
27	DX 3 Analog Channel 4 (or D-Wire 12 for unit with D-Wire support)	Voltage (VDC)	3
28	DX 3 Analog Channel 5 (or D-Wire 13 for unit with D-Wire support)	Voltage (VDC)	3
29	DX 3 Analog Channel 6 (or D-Wire 14 for unit with D-Wire support)	Voltage (VDC)	3

30	DX 3 Analog Channel 7 (or D-Wire 15 for unit with D-Wire support)	Voltage (VDC)	3
31	DX 3 Analog Channel 8 (or D-Wire 16 for unit with D-Wire support)	Voltage (VDC)	3

Analog Change Event

Obj 32 Var 01 - 32-Blt Analog Change Event Without Time
Class 2 Response

Will report only when an Analog value has crossed a threshold.

15 Frequently Asked Questions

Here are answers to some common questions from NetGuardian users. The latest FAQs can be found on the NetGuardian support web page, **http://www.dpstelecom.com.**

If you have a question about the NetGuardian, please call us at **(559) 454-1600** or e-mail us at **support@dpstele.com**

15.1 General FAQs

Q. How do I telnet to the NetGuardian?

A. You must use **Port 2002** to connect to the NetGuardian. Configure your Telnet client to connect using TCP/IP (**not** "Telnet," or any other port options). For connection information, enter the IP address of the NetGuardian and Port 2002. For example, to connect to the NetGuardian using the standard Windows Telnet client, click Start, click Run, and type "telnet <NetGuardian IP address> 2002."

Q. How do I connect my NetGuardian to the LAN?

A. To connect your NetGuardian to your LAN, you need to configure the unit IP address, the subnet mask and the default gateway. A sample configuration could look like this:
Unit Address: 192.168.1.100
subnet mask: 255.255.255.0
Default Gateway: 192.168.1.1
Save your changes by writing to NVRAM and reboot. Any change to the NetGuardian's IP configuration requires a reboot.

Q. When I connect to the NetGuardian through the craft port on the front panel it either doesn't work right or it doesn't work at all. What's going on?

A. Make sure your using the right COM port settings. Your COM port settings should read:
Bits per second: 9600 (9600 baud)
Data bits: 8
Parity: None
Stop bits: 1
Flow control: None
Important! Flow control **must** be set to **none**. Flow control normally defaults to hardware in most terminal programs, and this will not work correctly with the NetGuardian.

Q. I can't change the craft port baud rate.

A. If you select a higher baud rate, you must set your terminal emulator program to the new baud rate, press Enter, and type in your password. If your terminal emulator is set to a slower baud rate than the craft port, normal keys can appear as a break key - and the craft port interprets a break key as an override that resets the baud rate to the standard 9600 baud.

Q. How do I use the NetGuardian to access TTY interfaces on remote site equipment?

A. If your remote site device supports RS-232, you can connect it to one of the eight data ports located on the NetGuardian back panel. To make the data port accessible via LAN, configure the port for TCP/IP operation. You now have a LAN-based proxy port connection that lets you access your device's TTY interface through a Telnet session.

Q. I just changed the port settings for one of my data ports, but the changes did not seem to take effect even after I wrote the NVRAM.

A. In order for data port and craft port changes (including changes to the baud rate and word format) to take

effect, the NetGuardian must be rebooted. Whenever you make changes, remember to write them to the NetGuardian's NVRAM so they will be saved when the unit is rebooted.

Q. The LAN link LED is green on my NetGuardian, but I can't poll it from my T/Mon.

A. Some routers will not forward packets to an IP address until the MAC address of the destination device has been registered on the router's Address Resolution Protocol (ARP) table. Enter the IP address of your gateway and your T/Mon system to the ARP table.

Q. What do the terms "port," "address," "display" and "alarm point" mean?

A. These terms refer to numbers that designate the location of a network alarm, from the most general (a port to which several devices are connected) to the most specific (an individual alarm sensor).

Port: A number designating a serial port through which a monitoring device collects data.

Address: A number designating a device connected to a port.

Display: A number designating a logical group of 64 alarm points.

Alarm Point: A number designating a contact closure that is activated when an alarm condition occurs. For example, an alarm point might represent a low oil sensor in a generator or an open/close sensor in a door.

These terms originally referred only to physical things: actual ports, devices, and contact closures. For the sake of consistency, port-address-display-alarm point terminology has been extended to include purely logical elements: for example, the NetGuardian reports internal alarms on Port 99, Address 1.

Q. What characteristics of an alarm point can be configured through software? For instance, can point 4 be used to sense an active-low signal, or point 5 to sense a level or a edge?

A. The NetGuardian's standard configuration is for all alarm points to be level-sensed. You **cannot** use configuration software to convert alarm points to TTL (edge-sensed) operation. TTL alarm points are a hardware option that must be specified when you order your NetGuardian. Ordering TTL points for your NetGuardian does not add to the cost of the unit What you can do with the configuration software is change any alarm point from "Normal" to "Reversed" operation. Switching to Reversed operation has different effects, depending on the kind of input connected to the alarm point:

- **If the alarm input generates an active-high signal,** switching to Reversed operation means the NetGuardian will declare an alarm in the absence of the active-high signal, creating the practical equivalent of an active-low alarm.
- **If the alarm input generates an active-low signal,** switching to Reversed operation means the NetGuardian will declare an alarm in the absence of the active-low signal, creating the practical equivalent of an active-high alarm.
- **If the alarm input is normally open,** switching to Reversed operation converts it to a normally closed alarm point.
- **If the alarm input is normally closed,** switching to Reversed operation converts it to a normally open alarm point.

Q. Every time my NetGuardian starts up, I have to reenter the date and time. How can I get the NetGuardian to automatically maintain the date and time setting?

A. You have three options for keeping the correct time on your NetGuardian:

Real Time Clock Option: You can order your NetGuardian with the Real Time Clock hardware option. Once it's set, the Real Time Clock will keep the correct date and time, regardless of reboots.

Network Time Protocol Synchronization: If your NetGuardian has Firmware Version 2.9F or later, you can configure the unit to automatically synchronize to a Network Time Protocol (NTP) server.

- To get the latest NetGuardian firmware, sign in to MyDPS at www.dpstelecom.com/mydps.
- For instructions on configuring your NetGuardian to use NTP synchronization, see the "Network Time Protocol Support" section of this manual.

T/Mon RTU Time Sync Signal: You can configure your T/Mon NOC to send an RTU Time Sync signal at a regular interval, which you can set to any time period between 10 and 10,080 minutes. The Time Sync will automatically synchronize the NetGuardian's clock to the T/Mon's clock. And if you set your T/Mon to NTP

synchronization, you'll make sure you have consistent, accurate time stamps throughout your monitoring network.

Q. How do I back up my NetGuardian configuration?

A. Use FTP

You can use File Transfer Protocol (FTP) to read and write configuration files to the NetGuardian's NVRAM, but you can't use FTP to edit configuration files.

15.2 SNMP FAQs

Q. How do I configure the NetGuardian to send traps to an SNMP manager? Is there a separate MIB for the NetGuardian? How many SNMP managers can the agent send traps to? And how do I set the IP address of the SNMP manager and the community string to be used when sending traps?

A. The NetGuardian begins sending traps as soon as the SNMP managers are defined. The NetGuardian MIB is included on the NetGuardian Resource CD. The MIB should be compiled on your SNMP manager. (**Note:** MIB versions may change in the future.) The unit supports 2 SNMP managers, which are configured by entering its IP address in the Trap Address field of Ethernet Port Setup. You can also configure up to eight secondary SNMP managers, which is configured by selecting the secondary SNMP managers as pager recipients. Community strings are configured globally for all SNMP managers. To configure the community strings, choose System from the Edit menu, and enter appropriate values in the Get, Set, and Trap fields.

Q. Does the NetGuardian support MIB-2 and/or any other standard MIBs?

A. The NetGuardian supports the bulk of MIB-2.

Q. Does the NetGuardian SNMP agent support both NetGuardian and T/MonXM variables?

A. The NetGuardian SNMP agent manages an embedded MIB that supports only the NetGuardian's RTU variables. The T/MonXM variables are included in the distributed MIB only to provide SNMP managers with a single MIB for all DPS Telecom products.

Q. How many traps are triggered when a single point is set or cleared? The MIB defines traps like "major alarm set/cleared," "RTU point set," and a lot of granular traps, which could imply that more than one trap is sent when a change of state occurs on one point.

A. Generally, a single change of state generates a single trap, but there are two exception to this rule. Exception 1: the first alarm in an "all clear" condition generates an additional "summary point set" trap. Exception 2: the final clear alarm that triggers an "all clear" condition generates an additional "summary point clear" trap.

Q. What does "point map" mean?

A. A point map is a single MIB leaf that presents the current status of a 64-alarm-point display in an ASCII-readable form, where a "." represents a clear and an "x" represents an alarm.

Q. The NetGuardian manual talks about eight control relay outputs. How do I control these from my SNMP manager?

A. The control relays are operated by issuing the appropriate set commands, which are contained in the DPS control grid. For more information about the set commands, see Appendix, "Display Mapping," in any of the NetGuardian software configuration guides.

Q. How can I associate descriptive information with a point for the RTU granular traps?

A. The NetGuardian alarm point descriptions are individually defined using the Web Browser or TTY interfaces.

Q. My SNMP traps aren't getting through. What should I try?

A. Try these three steps:

1. Make sure that the Trap Address (IP address of the SNMP manager) is defined. (If you changed the Trap Address, make sure you saved the change to NVRAM and rebooted.)
2. Make sure all alarm points are configured to send SNMP traps.
3. Make sure the NetGuardian and the SNMP manager are both on the network. Use the NetGuardian's ping command to ping the SNMP manager.

15.3 Pager FAQs

Q. Why won't my alpha pager work?

A. To configure the NetGuardian to send alarm notifications to an alpha pager, enter the **data** phone number for your pager in the Phone Number field. This phone number should connect to your pager service's modem. Then enter the PIN for your pager in the PIN/Rcpt/Port field. You don't need to enter anything in any of the other fields. If you still don't receive pages, try setting the Dial Modem Init string to ATS37=9. This will limit the NetGuardian's connection speed. Be sure to use the rpt debug feature, if needed.

Q. Numeric pages don't come in or are cut off in the middle of the message. What's wrong?

A. You need to set a delay between the time the NetGuardian dials your pager number and the time the NetGuardian begins sending the page message. You can set the delay in the Pager Number field, where you enter your pager number. First enter the pager number, then enter some commas directly after the number. Each comma represents a two-second delay. So, for example, if you wanted an eight-second delay, you would enter "555-1212,,,," in the Pager Number field.

Q. What do I need to do to set up e-mail notifications?

A. You need to assign the NetGuardian an e-mail address and list the addresses of e-mail recipients. Let's explain some terminology. An e-mail address consists of two parts, the user name (everything before the "@" sign) and the domain (everything after the "@" sign). To assign the NetGuardian an e-mail address, choose System from the Edit menu. Enter the NetGuardian's user name in the Name field (it can't include any spaces) and the domain in the Location field. For example, if the system configuration reads:

Name: netguardian
Location: proactive.com

Then e-mail notifications from the NetGuardian will be sent from the address "netguardian@proactive.com." The next step is to list the e-mail recipients. Choose Pagers from the Edit menu. For each e-mail recipient, enter his or her e-mail domain in the Phone/Domain field and his or her user name in the PIN/Rcpt/Port field. You must also enter the IP address of an SMTP server in the IPA field and configure the alarm point to use the pager you setup as email.

16 Technical Support

DPS Telecom products are backed by our courteous, friendly Technical Support representatives, who will give you the best in fast and accurate customer service. To help us help you better, please take the following steps before calling Technical Support:

1. Check the DPS Telecom website.
You will find answers to many common questions on the DPS Telecom website, at **http://www.dpstelecom.com/support/**. Look here first for a fast solution to your problem.

2. Prepare relevant information.
Having important information about your DPS Telecom product in hand when you call will greatly reduce the time it takes to answer your questions. If you do not have all of the information when you call, our Technical Support representatives can assist you in gathering it. Please write the information down for easy access. Please have your user manual and hardware serial number ready.

3. Have access to troubled equipment.
Please be at or near your equipment when you call DPS Telecom Technical Support. This will help us solve your problem more efficiently.

4. Call during Customer Support hours.
Customer support hours are Monday through Friday, from 7 A.M. to 6 P.M., Pacific time. The DPS Telecom Technical Support phone number is **(559) 454-1600**.

Emergency Assistance: *Emergency assistance is available 24 hours a day, 7 days a week. For emergency assistance after hours, allow the phone to ring until it is answered with a paging message. You will be asked to enter your phone number. An on-call technical support representative will return your call as soon as possible.*

17 End User lisence Agreement

All Software and firmware used in, for, or in connection with the Product, parts, subsystems, or derivatives thereof, in whatever form, including, without limitation, source code, object code and microcode, including any computer programs and any documentation relating to or describing such Software is furnished to the End User only under a non-exclusive perpetual license solely for End User's use with the Product.

The Software may not be copied or modified, in whole or in part, for any purpose whatsoever. The Software may not be reverse engineered, compiled, or disassembled. No title to or ownership of the Software or any of its parts is transferred to the End User. Title to all patents, copyrights, trade secrets, and any other applicable rights shall remain with the DPS Telecom.

DPS Telecom's warranty and limitation on its liability for the Software is as described in the warranty information provided to End User in the Product Manual.

End User shall indemnify DPS Telecom and hold it harmless for and against any and all claims, damages, losses, costs, expenses, obligations, liabilities, fees and costs and all amounts paid in settlement of any claim, action or suit which may be asserted against DPS Telecom which arise out of or are related to the non-fulfillment of any covenant or obligation of End User in connection with this Agreement.

This Agreement shall be construed and enforced in accordance with the laws of the State of California, without regard to choice of law principles and excluding the provisions of the UN Convention on Contracts for the International Sale of Goods. Any dispute arising out of the Agreement shall be commenced and maintained only in Fresno County, California. In the event suit is brought or an attorney is retained by any party to this Agreement to seek interpretation or construction of any term or provision of this Agreement, to enforce the terms of this Agreement, to collect any money due, or to obtain any money damages or equitable relief for breach, the prevailing party shall be entitled to recover, in addition to any other available remedy, reimbursement for reasonable attorneys' fees, court costs, costs of investigation, and other related expenses.

*"**D**ependable, **P**owerful **S**olutions*
that allow users to monitor larger,
more complicated networks with a
smaller, less trained staff"

DPS Telecom
"Your Partners in Network Alarm Management"
www.dpstelecom.com
4955 E Yale • Fresno, CA 93727
559-454-1600 • 800-622-3314 • 559-454-1688 fax